Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Unidad Iztapalapa

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

Propiedades aditivas en subconjuntos de los residuos cuadráticos

Tesis que presenta

Rocío Meza Moreno

Para obtener el grado de

Doctora en Ciencias (Matemáticas)

Asesor: Dr. Mario Pineda Ruelas

Jurado calificador:

Presidente: Dr. Pedro Luis del Ángel Rodríguez

Secretario: Dr. Rogelio Fernández-Alonso González

Vocales: Dr. Mario Pineda Ruelas

Dr. Carlos José Enrique Signoret Poillon

Dra. Rita Esther Zuazua Vega

México, D. F., 9 de octubre de 2015

Propiedades aditivas en subconjuntos de los residuos cuadráticos

Rocío Meza Moreno
Posgrado en Matemáticas
Universidad Autónoma Metropolitana

Agradecimientos

y eso tal vez ocurra porque no sé ser otro
que ese otro que soy para los otros.
-Otherness, Mario Benedetti-

Cuando se culmina una etapa, es natural tomarse un tiempo para reflexionar un poco sobre cómo fue el trayecto. Recordamos las cosas buenas, las malas, los baches en el camino, los bloqueos, los momentos divertidos... y es inevitable pensar en aquellos que, de alguna u otra forma, nos acompañaron durante el proceso. Claro que las personas a las que debemos agradecer algo son siempre demasiadas, pero quiero aprovechar este espacio para mencionar particularmente a algunas de ellas.

Agradezco a mi familia por estar siempre al pendiente: mamá, papá, hermanos, saben que los quiero mucho. Agradecimiento especial a Moisés por leer mi primer artículo y darme sus puntos de vista (a pesar de que no es su área, pero es que tiene muy buen inglés). A mi cuñada Araceli, quien se ha convertido en mi mejor amiga y siempre tiene un consejo adecuado y un oído paciente para cuando las cosas no salen como uno espera. A mi cuñada Marcela porque, aunque ella no lo sepa, es una gran fuente de inspiración para mí. A mi pequeño Deco, básicamente por ser él y por siempre decir cosas tiernas como «lo cuadrático es lo tuyo» o «¿ya eres la Doctora Rocío Meza Moreno?», pero también por incluirme en sus peticiones anuales a los reyes magos (quizás también debería agradecerle a ellos...).

A Alejandro Sánchez por acompañarme en tantas aventuras a lo largo de este tiempo, por las discusiones que tuvimos de tan diversos temas, por los problemas que resolvimos y por los que no salieron. Gracias por el apoyo y gracias por estar.

A mis compañeros del posgrado. Alejandro Aguilar, mi compañero de siempre, por aguantarme en las clases y ayudarme con las tareas, y sobre todo, por siempre estar dispuesto a despejar mis dudas. José Luis Cosme, que es un gran amigo que comparte lo que sabe y nunca te niega su ayuda. Francisco González, con quien compartí parte de mi estancia en el cubículo de posgrado, por haber estado ahí para platicar de otras cosas (hasta de probabilidad) cuando la mente necesitaba despejarse un poco.

A mis compañeros del coro por todos los momentos agradables, dentro y fuera de la UAM (esos palomazos en el metro nunca los voy a olvidar) y por ser tan lindos con Deco: Nancy, Erika, Wendy, Deisy, Dalia, Laura, Lucero, Nubia, Sac, Hugo, Daniel, Kevin, Armando, Kike, Francisco, Miguel, Giovanni, etc. Son bastantes así que seguramente estoy comentiendo algún olvido, ustedes disculparán. A la maestra Angélica Ramírez Cruz, de la que aprendí muchas cosas, ninguna de ellas relacionada con matemáticas, que hicieron mi segunda estancia en la UAM mucho más agradable.

A los miembros del jurado, Rita Zuazua, Pedro Luis del Ángel, Carlos Signoret y Rogelio Fernández-Alonso, por haber revisado el trabajo y por sus valiosos comentarios. A mi asesor, Mario Pineda, por haberme instruido, por la paciencia y por tener siempre muchas preguntas.

Finalmente, agradezco al Consejo Nacional de Ciencia y Tecnología por el apoyo económico recibido.

Índice general

Agradecimientos I

Introducción V

1. Preliminares 1
1.1. Propiedades de los residuos cuadráticos 1
1.2. Trasladados de $R_p \cup \{0\}$ en $\mathbb{F}_p$ 5
1.3. Orden 8

2. Parejas y ternas de residuos cuadráticos consecutivos 13
2.1. Algunas propiedades 13
2.2. Parejas y ternas 16

3. Trasladados de algunos subconjuntos de R_p y N_p 23
3.1. Residuos en $R_{\frac{p-1}{2}} + a$ 23
3.2. Residuos en $N_{\frac{p-1}{2}} + a$ 39
3.3. Intersecciones de trasladados 47
3.4. Residuos en $R_{\frac{p-1}{4}} + a$ 50

4. Estimaciones 55
4.1. Sumas de Hua 55

Conclusiones 71

Bibliografía 73

Índice alfabético 75

Introducción

En el campo de los números reales determinar cuáles números son cuadrados es muy fácil: todo número real no negativo es un cuadrado. En $\mathbb{C}$, cualquier número es un cuadrado. Los cuadrados cobran relevancia en un campo con p elementos $\mathbb{F}_p$: aquí determinar cuáles números son cuadrados ya no es tan sencillo. Los cuadrados en este tipo de campos, llamados residuos cuadráticos, han sido ampliamente estudiados y se cuenta con diversos resultados importantes, destacando la *Ley de reciprocidad cuadrática*, conjeturada por Legendre y demostrada por Gauss. Entre las propiedades destacables del conjunto de residuos cuadráticos en $\mathbb{F}_p$ se encuentra el hecho de que son el único subgrupo máximo multiplicativo de $\mathbb{F}_p^*$, con todas las ventajas que eso implica. Sin embargo, la suma de residuos tiene un comportamiento totalmente distinto y las investigaciones en $\mathbb{F}_p^*$ desde el punto de vista algebraico que se encuentran en la literatura sobre sus propiedades aditivas no son abundantes ([6], [10], [11]). Algunas investigaciones, guiadas por los resultados de Perron [10], han obtenido resultados importantes en un campo finito $\mathbb{F}_{p^n}$ usando caracteres [14].

Cabe destacar que en lo que a distribución de cuadrados se refiere, el comportamiento es muy distinto para primos de la forma $p = 4k + 1$ y para primos de la forma $p = 4k - 1$. Para el primer tipo de primos, los cuadrados se distribuyen simétricamente porque a es residuo cuadrático si y solo si $-a$ lo es. Esto deriva en el hecho de que para un primo de la forma $p = 4k + 1$, entre 1 y $\dfrac{p-1}{2}$ hay la misma cantidad de residuos cuadráticos que de no residuos. Sin embargo, para un primo de la forma $p = 4k - 1$ la cantidad de cuadrados en este mismo intervalo es mayor que la cantidad de no cuadrados. Esto se debe a que el número de clases de ideales de un campo de números es un entero $h \geq 1$ y a la relación que hay entre h y la cantidad de residuos y no residuos cuadráticos entre 1 y $\dfrac{p-1}{2}$. Dicha relación viene dada por un resultado que aparece en [4] (teorema 4, página 346), y que es parte de la famosa fórmula analítica del número de clase de Dirichlet, que asegura que para un primo de la forma $p = 4k - 1 > 3$, el número de clase del campo cuadrático imaginario

$\mathbb{Q}(\sqrt{-p})$ satisface

$$h = \begin{cases} r_{\frac{p-1}{2}} - n_{\frac{p-1}{2}} & \text{si} \quad p \equiv 7 \pmod 8, \\ \frac{1}{3}(r_{\frac{p-1}{2}} - n_{\frac{p-1}{2}}) & \text{si} \quad p \equiv 3 \pmod 8, \end{cases}$$

donde $r_{\frac{p-1}{2}}$ y $n_{\frac{p-1}{2}}$ denotan, respectivamente, la cantidad de residuos y no residuos entre 1 y $\dfrac{p-1}{2}$. Esta fórmula se deduce directamente de la igualdad

$$h = \frac{1}{2 - \left(\frac{2}{p}\right)} \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

De acuerdo a Borevich-Shafarevich, se conoce una prueba de la afirmación anterior con argumentos puramente aritméticos para $p \equiv 3 \pmod 8$ [13], quedando sin prueba el caso $p \equiv 7 \pmod 8$. En 1978 aparece una prueba del caso faltante y con argumentos aritméticos en [9]. Localizar números primos o residuos cuadráticos es un problema abierto, y en ese orden de ideas se encuentra el Teorema de los Números primos el cual «solo» hace una estimación de la cantidad de primos menores o iguales que una cota dada.

El objetivo de este trabajo es estudiar dos aspectos de los residuos cuadráticos desde un punto de vista algebraico o aritmético: distribución y propiedades aditivas. Nuestro punto de partida es el célebre artículo de Oskar Perron [10]. Para p un primo impar sea $R_p^\dagger$ el conjunto de residuos cuadráticos módulo p incluyendo al 0, y $N_p = \mathbb{F}_p \setminus R_p^\dagger$. Perron determina el número de residuos cuadráticos y de no residuos en los conjuntos $R_p^\dagger + a$ y $N_p + a$, donde $a \in \mathbb{F}_p^*$, en particular, si $a = 1$ sus resultados dan el número de parejas de residuos cuadráticos y no residuos consecutivos; todo esto se presenta con detalle en el primer capítulo. En el segundo capítulo obtenemos explícitamente una terna de residuos cuadráticos consecutivos para cierto tipo de primos y diferente de las únicas dos conocidas [2], [12]. La parte medular del trabajo se encuentra en el tercer capítulo, en donde siguiendo a Perron nos preguntamos qué le sucede al número de residuos cuadráticos cuando trasladamos subconjuntos de $R_p^\dagger$ o N_p: calculamos explícitamente la cantidad de residuos y no residuos en algunos subconjuntos trasladados de los residuos y los no residuos. Incluimos ejemplos de los resultados obtenidos. Finalmente, en el cuarto capítulo usamos las sumas de Hua para obtener algunas estimaciones sobre la suma de cuadrados.

CAPÍTULO 1

Preliminares

1.1. Propiedades de los residuos cuadráticos

En el curso de este trabajo p es un número primo impar, $\mathbb{F}_p$ denota el campo finito de cardinalidad p y como siempre $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Puesto que $\mathbb{F}_p^*$ es un grupo multiplicativo de orden $p-1$, por el teorema de Lagrange tenemos que para $x \in \mathbb{F}_p^*$ se cumple $x^{p-1} \equiv 1 \pmod{p}$. Este resultado es el famoso Teorema Pequeño de Fermat. Si $a \in \mathbb{F}_p^*$, diremos que a es un residuo cuadrático en $\mathbb{F}_p$ si la congruencia $x^2 \equiv a \pmod{p}$ es soluble. En caso contrario diremos que a es un no residuo cuadrático. La función $\left(\frac{-}{p}\right) : \mathbb{F}_p^* \to \{1, -1\}$ definida como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \pmod{p} \text{ es soluble,} \\ -1 & \text{si } x^2 \equiv a \pmod{p} \text{ no es soluble.} \end{cases}$$

es un homomorfismo de grupos en donde $ker\left(\frac{-}{p}\right) = \{a^2 : a \in \mathbb{F}_p^*\}$. De ahora en adelante, al grupo de residuos cuadráticos, $ker\left(\frac{-}{p}\right)$, lo denotaremos como R_p y $N_p = \mathbb{F}_p^* \setminus R_p$. La función $\left(\frac{-}{p}\right)$ se conoce como el símbolo de Legendre. En todos los capítulos de este trabajo escribiremos $[\![1, n]\!] = \{1, 2, \cdots, n\}$. El siguiente resultado resume en buena medida las propiedades fundamentales del símbolo de Legendre.

Teorema 1.1.1. *Sean $a, b \in \mathbb{Z}$, p primo impar con* $\text{mcd}(ab, p) = 1$. *Entonces:*

1. *Si $a \equiv b \pmod{p}$, entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ *(teorema de Euler).*

3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Demostración. Es inmediata. □

Corolario 1.1.1. *Para p un primo impar, se tiene que* $|R_p| = \frac{p-1}{2}$.

Demostración. Se sigue de observar que $\mathbb{F}_p^*/ker\left(\frac{-}{p}\right) \simeq \{-1, 1\}$. □

Notamos que exactamente la mitad de los elementos de $\mathbb{F}_p^*$ son un cuadrado. El número -1 no es un cuadrado en los campos $\mathbb{Q}$ y $\mathbb{R}$ pero en campos finitos de cardinalidad p, con p un primo, tenemos que:

Teorema 1.1.2. *$-1 \in R_p$ si y solo si $p = 2$ o $p = 4k + 1$.*

Demostración. Supongamos que $p \neq 2$ y $p \not\equiv 1 \pmod{4}$. Sea x tal que $x^2 \equiv -1 \pmod{p}$. En este caso $\frac{p-1}{2}$ es impar y por el Teorema Pequeño de Fermat tenemos que

$$x^{p-1} \equiv 1 \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

lo cual no es posible pues $p \neq 2$ y así $p \equiv 1 \pmod{4}$. Recíprocamente, si $p = 4k + 1$, entonces $\frac{p-1}{2}$ es par. El teorema de Wilson nos asegura que $(p-1)! \equiv -1 \pmod{p}$ y y por lo tanto el número $(-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j$ satisface $x^2 \equiv -1 \pmod{p}$. □

Corolario 1.1.2. *Sea $p \equiv 1 \mod 4$ un primo. Entonces* $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$.

Demostración. La afirmación se sigue de observar que si b es solución de $x^2 \equiv a \pmod{p}$ y x es tal que $x^2 \equiv -1 \pmod{p}$, entonces xb es solución de $x^2 \equiv -a \pmod{p}$. □

El corolario anterior nos permite afirmar que si $p \equiv 1 \pmod{4}$, entonces en el conjunto $1, 2, \ldots, \frac{p-1}{2}$ también la mitad de sus elementos son un cuadrado.

Teorema 1.1.3. *Si $p \equiv 1 \pmod 4$ es un primo, entonces* $\sum_{n=1}^{\frac{p-1}{2}} \left(\frac{n}{p}\right) = 0.$

Demostración. De acuerdo al corolario anterior, la mitad de los residuos cuadráticos de $\mathbb{F}_p$ se encuentra entre 1 y $\frac{p-1}{2}$. □

Un hecho conocido es la naturaleza cuadrática de los números 2 y 3.

Teorema 1.1.4. *Sea p un primo impar. Entonces*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{si y solo si} \quad p \equiv 1, 7 \pmod 8, \\ -1 & \textit{si y solo si} \quad p \equiv 3, 5 \pmod 8. \end{cases}$$

Para $p \neq 3$,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{si y solo si } p \equiv 1, 11 \pmod{12}, \\ -1 & \textit{si y solo si } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Un problema no resuelto en la teoría de residuos cuadráticos es la distribución de los cuadrados en el campo $\mathbb{F}_p$, es decir, ¿en dónde se encuentran localizados los cuadrados?. Podemos localizar algunos de ellos.

Teorema 1.1.5. *Si $p = 2k + 1$ es un primo impar, entonces*

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \textit{si y solo si} \quad p \equiv 1, 3 \pmod 8, \\ -1 & \textit{si y solo si} \quad p \equiv 5, 7 \pmod 8. \end{cases}$$

Demostración. Puesto que $\left(\frac{-1}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{k}{p}\right)$, tenemos

$$\left(\frac{k}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right).$$

Por lo anterior, $\left(\frac{k}{p}\right) = 1$ si y solo si $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)$. Así que

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si y solo si} \quad p \equiv 1 \pmod 8, \\ -1 & \text{si y solo si} \quad p \equiv 3 \pmod 8. \end{cases}$$

Finalmente observemos que $\left(\frac{k}{p}\right) = -1$ si y solo si $\left(\frac{2}{p}\right) = -\left(\frac{-1}{p}\right)$. Por lo tanto

$$\left(\frac{2}{p}\right) = -\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si y solo si} \quad p \equiv 7 \pmod 8, \\ -1 & \text{si y solo si} \quad p \equiv 5 \pmod 8. \end{cases}$$

□

Como caso particular, si $p = 4k + 1$ el resultado anterior tiene la siguiente interpretación:

Corolario 1.1.3. *Si* $p \equiv 1 \pmod 4$ *es un primo, entonces*

$$\left(\frac{\frac{p-1}{2}}{p}\right) = \begin{cases} 1 & \text{si y solo si} \quad p \equiv 1 \pmod 8, \\ -1 & \text{si y solo si} \quad p \equiv 5 \pmod 8. \end{cases}$$

□

Una consecuencia del corolario anterior es que, para esta misma clase de primos, $\left(\frac{\frac{p-1}{2}}{p}\right) = \left(\frac{2}{p}\right)$.

Corolario 1.1.4. *Si* $p \equiv 1 \pmod 4$ *es primo, entonces* $\left(\frac{\frac{p+1}{2}}{p}\right) = \left(\frac{\frac{p-1}{2}}{p}\right)$.

Demostración. Como $1 = \left(\frac{1}{p}\right) = \left(\frac{p+1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{p+1}{2}}{p}\right)$, entonces $\left(\frac{2}{p}\right) = \left(\frac{\frac{p+1}{2}}{p}\right)$ y del comentario anterior se sigue el resultado. □

Teorema 1.1.6. *Si* $p = 4k + 1$ *es un número primo, entonces*

1. $\left(\frac{k}{p}\right) = 1$.

2. *Si* k *es par, entonces* $\left(\frac{\frac{k}{2}}{p}\right) = 1$.

Demostración. Primero notemos que $\left(\frac{k}{p}\right) = \left(\frac{4k}{p}\right) = \left(\frac{-1}{p}\right) = 1$. Para la segunda afirmación supongamos $p = 8t + 1$. Entonces $\left(\frac{2}{p}\right) = 1$ y por tanto para $j \in \mathbb{Z}$ se tiene $\left(\frac{2^j}{p}\right) = 1$. Por lo anterior $\left(\frac{8^{-1}}{p}\right) = 1$. Así que

$$\left(\frac{\frac{k}{2}}{p}\right) = \left(\frac{\frac{p-1}{8}}{p}\right) = \left(\frac{(p-1)8^{-1}}{p}\right) = \left(\frac{p-1}{p}\right)\left(\frac{8^{-1}}{p}\right) = 1.$$

□

1.2. Trasladados de $R_p \cup \{0\}$ en $\mathbb{F}_p$

Sabemos que el problema de localizar residuos cuadráticos es un problema abierto y la teoría analítica de los números ha hecho contribuciones importantes en esta dirección. Sin embargo, todas esas contribuciones no son explícitas y por tanto, aunque no podamos localizarlos, intentaremos contarlos. En este orden de ideas, Perron en [10], hace un estudio exitoso en el campo finito $\mathbb{F}_p$. En esta sección desarrollamos las ideas principales de Perron, pues estas serán la guía espiritual de los siguientes capítulos.

En la siguiente discusión p representa un primo impar y R_p denota al grupo de residuos cuadráticos módulo p, en donde $|R_p| = \dfrac{p-1}{2}$.

Primero que nada, notemos que R_p tiene la siguiente propiedad: si $x \in R_p$, entonces $xR_p = R_p$, y si $x \notin R_p$, con $x \neq 0$, entonces xR_p reproduce a todos los no residuos cuadráticos en $\mathbb{F}_p^*$. El grupo R_p es el único subgrupo de $\mathbb{F}_p^*$ de índice 2. Con respecto a la adición podemos preguntarnos lo siguiente: sea $a \in \mathbb{F}_p^*$, ¿podemos identificar los residuos cuadráticos en el trasladado $R_p + a$?. La pregunta es difícil de responder pues tiene que ver con la distribución de los cuadrados en $\mathbb{F}_p$. El célebre teorema de Perron calcula explícitamente el número de residuos y no residuos en el trasladado $R_p + a$.

Teorema 1.2.1 (Perron)**.** *Sean $p = 4k-1$ un primo y $R_p^\dagger = \{r_1, r_2, \ldots, r_{2k}\}$ el conjunto de residuos cuadráticos incluyendo al 0. Si $a \in \mathbb{F}_p^*$, entonces $|(R_p^\dagger + a) \cap R_p^\dagger| = k$. Sean $p = 4k+1$ un primo y $R_p^\dagger = \{r_1, r_2, \ldots, r_{2k+1}\}$ los residuos cuadráticos incluyendo al 0. Si $a \in R_p$, entonces $|(R_p^\dagger + a) \cap R_p^\dagger| = k+1$ y si $a \in N_p$, tenemos $|(R_p^\dagger + a) \cap R_p^\dagger| = k$.*

Demostración. Escribimos $r_v \equiv s_v^2$. Si $r_v + a \in R_p^\dagger$, entonces $r_v + a \equiv s_v^2 + a \equiv t_v^2$ (mód p) y módulo p tenemos

$$s_v^2 - t_v^2 \equiv -a, \quad s_v - t_v \equiv -\frac{a}{s_v + t_v}, \quad 2s_v \equiv s_v + t_v - \frac{a}{s_v + t_v}.$$

Si $u = s_v + t_v$, entonces $s_v \equiv \dfrac{1}{2}\left(u - \dfrac{a}{u}\right)$ (mód p). Resumiendo: $r_v + a \in R_p^\dagger$ si existe $u \in \mathbb{F}_p^*$ tal que $s_v \equiv \dfrac{1}{2}\left(u - \dfrac{a}{u}\right)$ (mód p). La condición también es suficiente. En efecto, si $s_v \equiv \dfrac{1}{2}\left(u - \dfrac{a}{u}\right)$ (mód p) y hacemos $t \equiv \dfrac{1}{2}\left(u + \dfrac{a}{u}\right)$, entonces $s_v \equiv t - \dfrac{a}{u}$ (mód p) y $u = t + s_v$. Por lo anterior $\dfrac{a}{u} \equiv t - s_v$. Así que

$$a \equiv u\,\frac{a}{u} \equiv (t + s_v)(t - s_v) \equiv t^2 - s_v^2 \quad (\text{mód } p),$$

y por lo tanto $s_v^2 + a \in R_p^\dagger$. Hemos visto que para r_v un residuo cuadrático, el número $r_v + a$ también es residuo cuadrático si y solo si

$$r_v = \frac{1}{4}\left(u - \frac{a}{u}\right)^2$$

para algún $u \in \mathbb{F}_p^*$. Debemos pues contar cuántos residuos de la forma $\left(u - \frac{a}{u}\right)^2$ son incongruentes entre sí. Dado u, la congruencia

$$\left(x - \frac{a}{x}\right)^2 \equiv \left(u - \frac{a}{u}\right)^2 \pmod{p} \qquad (2)$$

tiene soluciones:

$$x = u \quad x = -u, \quad x = \frac{a}{u}, \quad x = -\frac{a}{u} \qquad (3)$$

Notamos que $\frac{a}{u} \not\equiv -\frac{a}{u} \pmod{p}$ y $u \not\equiv -u \pmod{p}$. Por lo anterior, (2) admite al menos dos soluciones incongruentes pero esto último no garantiza que las 4 soluciones sean incongruentes. Veamos la justificación de la primera afirmación del teorema. Supongamos que $p = 4k - 1$. En este caso, solo uno de los números a o $-a$ es un cuadrado. Observemos lo siguiente:

i) Si $a \in R_p$ y $u \in \mathbb{F}_p^*$ es tal que $u^2 \equiv a \pmod{p}$, entonces (2) solo tiene dos soluciones incongruentes. Esto es porque $u \equiv \frac{a}{u} \pmod{p}$.

ii) Si $a \in R_p$ y $u_1 \in \mathbb{F}_p^* \setminus \{\pm u\}$, entonces $\left(x - \frac{a}{x}\right)^2 \equiv \left(u_1 - \frac{a}{u_1}\right)^2 \pmod{p}$ tiene cuatro soluciones incongruentes.

iii) Si $a \in N_p$, entonces $-a \in R_p$ y por lo tanto, la afirmación en i) también aplica para $-a$. En este caso $u \equiv -\frac{a}{u} \pmod{p}$.

iv) Puesto que $\left(u - \frac{a}{u}\right)^2 = \left(-u - \frac{a}{-u}\right)^2$, tenemos que u y $-u$ producen el mismo elemento de R_p.

v) Puesto que $\left(\frac{a}{u} - \frac{a}{\frac{a}{u}}\right)^2 = \left(-\frac{a}{u} - \frac{a}{-\frac{a}{u}}\right)^2$, tenemos que $\frac{a}{u}$ y $-\frac{a}{u}$ producen el mismo elemento de R_p.

Sea $a \in R_p$ y u como en i). Para $u_1 \in \mathbb{F}_p^* \setminus \{u, -u\}$, tenemos que cada elemento de (3) produce el mismo cuadrado. Así que cada uno de los $4k-2-2$ elementos de $\mathbb{F}_p^* \setminus \{u, -u\}$ produce exactamente el mismo cuadrado de cuatro maneras diferentes, de modo que hay $\dfrac{4k-4}{4}$ cuadrados de la forma $r_v + a$, con $r_v \in R_p^\dagger$. Pero debemos añadir un 1 a nuestra cuenta porque falta considerar el cuadrado que se obtiene con u, que en este caso es 0. Por lo anterior, la cantidad de cuadrados en $R_p^\dagger + a$ es $1 + \dfrac{4k-4}{4} = k$. Si $a \in N_p$, entonces la congruencia (2) y la afirmación (3) también son válidas y se aplican los mismos argumentos para justificar que $|(R_p^\dagger + a) \cap R_p| = k$.

Ahora demostraremos la segunda afirmación del teorema. Supongamos que $p = 4k+1$. Distinguimos dos casos: $a \in N_p$ y $a \in R_p$. Si $a, -a \in N_p$, entonces las cuatro soluciones (3) de (2) son incongruentes, de modo que cada $u \in \mathbb{F}_p^*$ produce cuatro veces el mismo cuadrado. Por lo tanto $R_p^\dagger + a$ contiene $\dfrac{4k}{4} = k$ cuadrados.

Para el caso $a \in R_p$ consideremos $u_1, -u_1 \in \mathbb{F}_p^*$ tales que $u_1^2 \equiv (-u_1)^2 \equiv a \pmod{p}$. Para este u_1 notamos que $u_1 \equiv \dfrac{a}{u_1} \pmod{p}$ o equivalentemente $-u_1 \equiv -\dfrac{a}{u_1} \pmod{p}$. Así que (2) solo tiene dos soluciones incongruentes: u_1 y $-u_1$. Además, estas dos soluciones producen el mismo cuadrado:

$$\left(u_1 - \frac{a}{u_1}\right)^2 \equiv \left(-u_1 - \frac{a}{-u_1}\right)^2 \equiv 0 \pmod{p}.$$

Lo mismo sucede con $-a$. Sean $u_2, -u_2 \in \mathbb{F}_p^*$ tales que $u_2^2 \equiv (-u_2)^2 \equiv -a \pmod{p}$. Entonces $u_2 \equiv -\dfrac{a}{u_2} \pmod{p}$ y $u_2, -u_2$ producen el mismo cuadrado:

$$\left(u_2 - \frac{a}{u_2}\right)^2 \equiv \left(-u_2 - \frac{a}{-u_2}\right)^2 \pmod{p}.$$

Es fácil ver que

$$\left(u_1 - \frac{a}{u_1}\right)^2 \not\equiv \left(u_2 - \frac{a}{u_2}\right)^2 \pmod{p}.$$

Sea $u \in \mathbb{F}_p^* \setminus \{\pm u_1, \pm u_2\}$. Entonces

$$\left(u - \frac{a}{u}\right)^2 \equiv \left(-u - \frac{a}{-u}\right)^2 \equiv \left(\frac{a}{u} - \frac{a}{\frac{a}{u}}\right)^2 \equiv \left(-\frac{a}{u} - \frac{a}{-\frac{a}{u}}\right)^2 \pmod{p},$$

así que para esta u tenemos que $u, -u, \dfrac{a}{u}, \dfrac{a}{-u}$ producen el mismo cuadrado. Ahora vamos a calcular cuántos residuos cuadráticos contiene $R_p^\dagger + a$. Cada $u \in \mathbb{F}^* \setminus$

$\{\pm u_1, \pm u_2\}$ produce 4 veces el mismo cuadrado, con lo cual obtenemos $\frac{4k-4}{4}$ cuadrados. Pero nos falta considerar dos cuadrados más, justamente los que producen u_1 y u_2. Así que $|(R_p^\dagger + a) \cap R_p| = 2 + \frac{4k-4}{4} = k+1$. □

Corolario 1.2.1. *Si $p = 4k-1$ es un número primo, entonces $|\left(R_p^\dagger + a\right) \cap N_p| = k$ para $a \in \mathbb{F}_p^*$. Si $p = 4k+1$ y $a \in R_p$, entonces $|\left(R_p^\dagger + a\right) \cap N_p| = k$ y si $a \in N_p$, entonces $|\left(R_p^\dagger + a\right) \cap N_p| = k+1$ no residuos.* □

Corolario 1.2.2. *Sean $p = 4k-1$ un número primo, $a \in \mathbb{F}_p^*$ y $N_p = \{n_1, n_2, \ldots n_{2k-1}\}$ el conjunto de no residuos cuadráticos en $\mathbb{F}_p$. Entonces $|(N_p + a) \cap R_p^\dagger| = k$.*

Corolario 1.2.3. *Sean $p = 4k+1$ un número primo, $a \in \mathbb{F}_p^*$ y $N_p = \{n_1, n_2, \ldots n_{2k}\}$ el conjunto de no residuos cuadráticos en $\mathbb{F}_p$. Si $a \in R_p$, entonces $|(N_p + a) \cap R_p^\dagger| = k$. Si $a \in N_p$, entonces $|(N_p + a) \cap R_p^\dagger| = k+1$.*

Un caso de particular importancia es la cantidad de residuos cuadráticos consecutivos en R_p, éstos se obtienen de manera sencilla al trasladar $R_p^\dagger$ con $a = 1$.

Corolario 1.2.4. *Si $p = 4k-1$ es un número primo, entonces existen k pares de residuos cuadráticos consecutivos (incluyendo el par $0, 1$) y $k-1$ pares de no residuos cuadráticos consecutivos.*

Demostración. En $R_p^\dagger + 1$ observemos que si $r_i + 1$ es residuo, entonces r_i y $r_i + 1$ son residuos consecutivos. De la primera afirmación del teorema 1.2.1 se sigue el resultado. □

Corolario 1.2.5. *Si $p = 4k+1$ es un número primo, entonces existen $k+1$ pares de residuos cuadráticos consecutivos (incluyendo los pares $0, 1$ y $p-1, 0$) y k pares de no residuos cuadráticos consecutivos.*

Demostración. Idéntica al corolario anterior. □

1.3. Orden

Estamos interesados en estimar el orden multiplicativo de ciertos elementos de $\mathbb{F}_p^*$. Obsérvese que, en general, $o(\frac{p-1}{a}) = o(-a^{-1})$, y como en un grupo multiplicativo se cumple $o(x) = o(x^{-1})$ entonces

$$\begin{aligned} o(-a) &= o\left((-a)^{-1}\right) \\ &= o\left((-1)^{-1}(a)^{-1}\right) \\ &= o\left(-a^{-1}\right). \end{aligned}$$

Así pues, determinar el orden de $\frac{p-1}{a}$ es equivalente a determinar el orden de $o(-a)$, el cual se puede poner en términos de $o(a)$. En efecto, surgen dos casos, si $-1 \in \langle a \rangle$, sea $n \in \mathbb{N}$ el menor entero tal que $-1 = a^n$, entonces $-a = a^{n+1}$ Tenemos pues que,

$$\begin{aligned}(-a)^{n+1} &= (-1)^{n+1}a^{n+1} \\ &= \begin{cases} a^{n+1} & \text{si } n \text{ es impar} \\ -a^{n+1} & \text{si } n \text{ es par} \end{cases} \\ &= \begin{cases} -a & \text{si } n \text{ es impar} \\ a & \text{si } n \text{ es par} \end{cases}\end{aligned}$$

Así, cuando n es impar, se tiene que $o(-a) = n$. Además, como $a^n = -1$, entonces $a^{2n} = 1$. Por lo tanto, $o(a) = 2n$, es decir, $o(a) = 2 \cdot o(-a)$ cuando n es impar. Por otro lado, si n es par entonces, $o(-a) = o(a)$ ya que, en este caso,

$$1 = a^{o(a)} = \left[(-a)^{n+1}\right]^{o(a)} = (-a^{n+1})^{o(a)} = (-1)^{o(a)}$$

lo cual significa que $o(a)$ es par, de modo que,

$$(-a)^{o(a)} = (-1)^{o(a)} \cdot a^{o(a)} = 1$$

y así, $o(-a) = o(a)$ como habíamos afirmado.

Ahora, si $-1 \notin \langle a \rangle$, entonces $o(a)$ debe ser impar, pues de lo contrario, $\langle a \rangle$ contendría al subgrupo de orden dos, a saber, $\langle -1 \rangle$. De este modo tenemos que $o(-1)$ y $o(a)$ son primos relativos y por tanto,

$$o(-a) = o(-1)o(a) = 2 \cdot o(a)$$

En síntesis, hemos probado

Proposición 1.3.1. *En $\mathbb{F}_p^*$, las siguientes afirmaciones son ciertas:*

1. *Si $-1 \notin \langle a \rangle$, entonces $o(-a) = 2 \cdot o(a)$.*
2. *Si $-1 \in \langle a \rangle$, y $-1 = a^n$, entonces*

$$o(-a) = \begin{cases} \dfrac{o(a)}{2} & \textit{si } n \textit{ es impar,} \\ o(a) & \textit{si } n \textit{ es par.} \end{cases}$$

Si $a = 4$ se presenta una situación especial, que se establece en el siguiente resultado.

Proposición 1.3.2. *Si $p \equiv 1 \pmod 4$ entonces $o(\frac{p-1}{4})$ es un divisor de $\frac{p-1}{4}$.*

Demostración. Recordemos primero que $o(\frac{p-1}{4}) = o(-4)$. Si $\left(\frac{2}{p}\right) = 1$, entonces $p \equiv 1 \pmod 8$ así que $\frac{p-1}{4}$ es par, además, por el criterio de Euler $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p$, así

$$(-4)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}}(4)^{\frac{p-1}{4}} \equiv (1)(2)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Por otro lado, si $\left(\frac{2}{p}\right) = -1$, entonces $p \equiv 5 \pmod 8$ así que $\frac{p-1}{4}$ es impar y por tanto

$$(-4)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}}(2)^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 \pmod p$$

En ambos casos $o(-4)$ divide a $\frac{p-1}{4}$, lo cual da el resultado. □

Teorema 1.3.1. *Sean $p = 4k+1$ un número primo y $g \neq g_1$ tales que $\langle g\rangle = \langle g_1\rangle = \mathbb{F}_p^*$.*

1. *Si $n, n_1 \in \mathbb{N}$ satisfacen $g^n = g_1^{n_1}$, entonces $n \equiv n_1 \pmod 4$.*
2. *$\langle g\rangle = \mathbb{F}_p^*$ si y solo si $\langle p-g\rangle = \mathbb{F}_p^*$.*
3. *Si $x = g^n = (p-g)^{n_1}$ y $x \in R_p$, entonces $n = n_1$.*
4. *Si $g^2 \equiv g_1^2 \pmod p$, entonces $g \equiv -g_1 \pmod p$.*

Demostración. Para la afirmación 1 primero observemos que $g = g_1^{2t+1}$. Entonces

$$g^n = g_1^{n(2t+1)} = g_1^{n_1}.$$

Por lo anterior $n(2t+1) \equiv n_1 \pmod{p-1}$. Si $n = 4a + r$ y $n_1 = 4b + r_1$, entonces $4k \mid (8at + 4a - 4b) + (2tr + r - r_1)$. Así que $r \equiv r_1 \pmod 2$; es decir, r y r_1 tienen la misma paridad y $r, r_1 \in \{0, 1, 2, 3\}$. Es claro que si $r \neq r_1$, entonces $4 \nmid 2tr + r - r_1$ y por tanto $r = r_1$.

Para la afirmación 2 notamos que $-1 \in \langle g\rangle$ y como $p = 4k + 1$, entonces -1 es un residuo cuadrático y por tanto $-1 = g^n$ con n par, así que de la proposición 1.3.1 se concluye que $o(g) = o(p-g)$, por lo que $p - g$ también genera $\mathbb{F}_p^*$.

Para la tercera afirmación observe que la hipótesis $x \in R_p$ implica que n y n_1 son ambos pares y sin pérdida de generalidad podemos suponer que $n, n_1 \in [\![1, p-1]\!]$. Así que

$$g^n = (p-g)^{n_1} = \sum_{i=0}^{n_1} (-1)^i p^{n_i - i} g^i \equiv (-1)^{n_1} g^{n_1} \equiv g^{n_1} \pmod p,$$

y por tanto $n = n_1$.

Para la afirmación 4, sea $n \in [\![2, p-2]\!]$ tal que $g_1 = g^n$. Entonces tenemos

$$0 \equiv g_1^2 - g^2 \equiv (g^n - g)(g^n + g) \pmod{p}$$

Lo cual se cumple si alguno de los factores es cero. Pero $g^n - g \not\equiv 0 \pmod{p}$ pues $n < p - 1 = o(g)$, por lo tanto debe de ocurrir que $g^n \equiv -g \pmod{p}$, lo cual da el resultado. □

Observe que la hipótesis $p = 4k + 1$ es imprescindible en la afirmación 2 del teorema anterior, pues para $p = 4k + 3$, $-1 \notin R_p$ así que la n de la proposición 1.3.1 es impar y por lo tanto $o(-g) = o(g)/2$. Por ejemplo, para $p = 19$ se tiene que $o(2) = 18$ y $o(p - 2) = o(17) = 9$.

La citada afirmación establece que para un primo $p = 4k + 1$, si g es un generador de $\mathbb{F}_p^*$ entonces $p - g$ también lo es. Es decir, si $x \in \mathbb{F}_p^*$, existen $n, n_1 \in [\![1, p-1]\!]$ tales que $x = g^n = (p - g)^{n_1}$. A continuación establecemos una relación explícita entre n y n_1.

Si n es par, es claro que $(p - g)^n = g^n = x$. Si n es impar y $n \geq \dfrac{p-1}{2}$ entonces

$$(p-g)^{n-\frac{p-1}{2}} \equiv (-g)^n(-g)^{-\frac{p-1}{2}} \equiv -g^n(p-1)^{-1} = g^n \pmod{p}.$$

Si $n < \dfrac{p-1}{2}$, entonces

$$(p-g)^{n+\frac{p-1}{2}} \equiv (-g)^n(-g)^{\frac{p-1}{2}} \equiv (-1)g^n(p-1) = g^n \pmod{p}.$$

Así, tenemos la siguiente consecuencia

Corolario 1.3.3. *Sea $p = 4k + 1$. Si $\langle g \rangle = \mathbb{F}_p^*$ y $x = g^n$ para algún $n \in [\![1, p-1]\!]$, entonces*

1. *Si $x \in R_p$, entonces $x = g^n = (p - g)^n$.*
2. *Si $x \in N_p$, entonces*

$$x = g^n = \begin{cases} (p-g)^{n-\frac{p-1}{2}} & \text{si } n \geq \frac{p-1}{2}, \\ (p-g)^{n+\frac{p-1}{2}} & \text{si } n < \frac{p-1}{2}. \end{cases}$$

□

CAPÍTULO 2

Parejas y ternas de residuos cuadráticos consecutivos

2.1. Algunas propiedades

Como ya se dijo, (corolario 1.1.2) para primos de la forma $p \equiv 1 \mod 4$, el símbolo de Legendre satisface

$$\left(\frac{n}{p}\right) = \left(\frac{p-n}{p}\right).$$

Esto significa que para esta clase de primos los residuos cuadráticos en $[\![1, p-1]\!]$ presentan una especie de simetría: n es residuo cuadrático si y solo si $p-n$ también lo es. En los sucesivo llamaremos a esta propiedad la *simetría elemental* . La figura 2.1 muestra una representación gráfica de esta idea.

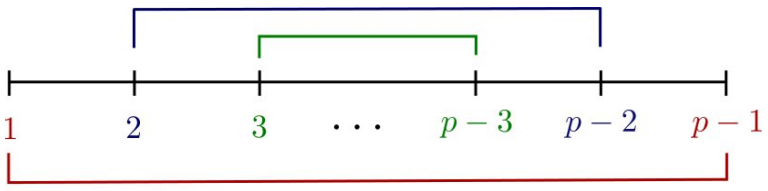

Figura 2.1: Simetría de los residuos cuadráticos en $\mathbb{F}_p$.

Ahora, si para un primo de esta misma forma, consideramos el intervalo discreto $[\![1, \frac{p-1}{2}]\!]$, el teorema 1.1.3 nos indica que la propiedad de tener la misma cantidad de residuos cuadráticos que de no residuos se sigue cumpliendo. Sin embargo, es claro

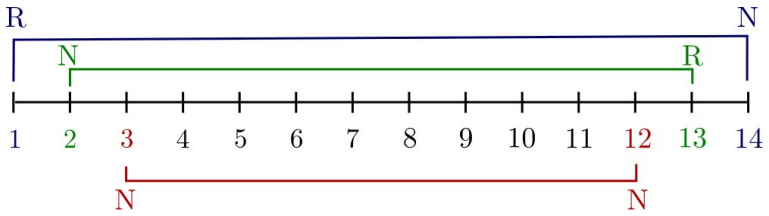

Figura 2.2: No simetría de los residuos cuadráticos en $[\![1, \frac{p-1}{2}]\!]$.

que la simetría elemental se pierde. En la figura 2.2 se ilustra un ejemplo para el primo $p = 29$.

Si consideramos un intervalo de valores aún más pequeño, por ejemplo, $[\![1, \frac{p-1}{4}]\!]$ es natural esperar que se pierdan más propiedades respecto a la forma en que se distribuyen los residuos cuadráticos. En efecto, no solo se pierde la simetría que se tenía en todo $\mathbb{F}_p$ sino que en dicho intervalo ya no se tiene la misma cantidad de residuos cuadráticos que de no residuos, como ocurría en los dos intervalos mencionados antes. Aunque se sabe que en $[\![1, \frac{p-1}{4}]\!]$ hay más residuos cuadráticos que no residuos módulo $p \equiv 1 \pmod 4$ [3], no conocemos una demostración con argumentos puramente aritméticos. A continuación veremos una serie de resultados que permiten relacionar algunos residuos cuadráticos en $\mathbb{F}_p$.

Proposición 2.1.1. *Si $p = 4k + 1$ es un número primo, entonces para $n \in \mathbb{Z}$ se cumple*

$$\left(\frac{\frac{p-1}{2} - n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2n+1}{p}\right).$$

Demostración. Tenemos que $\left(\frac{p-1-2n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{p-1-2n}{2}}{p}\right)$. Por la simetría elemental

$$\left(\frac{\frac{p-1}{2} - n}{p}\right) = \left(\frac{\frac{p-1-2n}{2}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p-(2n+1)}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2n+1}{p}\right).$$

□

La proposición anterior puede interpretarse como sigue. Si $p \equiv 1 \pmod 8$, entonces los números $\frac{p-1}{2} - n$ y $2n + 1$ son ambos residuos o ambos no residuos cuadráticos módulo p y si $p \equiv 5 \pmod 8$ entonces uno de dichos números es un residuo y el otro es un no residuo. Esto da una correspondencia entre los números $\frac{p-1}{2} - n$ y $2n + 1$ que se ilustra en la figura 2.3.

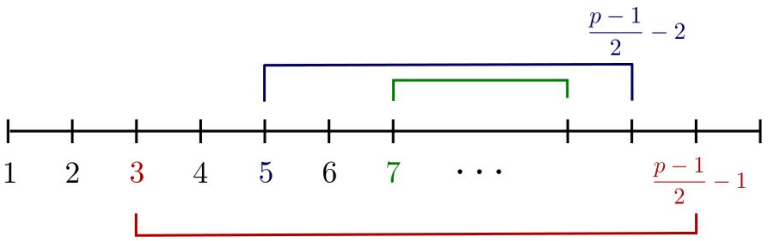

Figura 2.3: Correspondencia dada por la proposición 2.1.1.

Siguiendo las mismas ideas en la demostración de la proposición 2.1.1, se obtiene el siguiente resultado que es muy similar y cuya interpretación se ilustra en la figura 2.4.

Proposición 2.1.2. *Si $p = 4k + 1$ es un número primo, entonces para $n \in \mathbb{Z}$ se tiene que*

$$\left(\frac{\frac{p-1}{2}+n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2n-1}{p}\right).$$

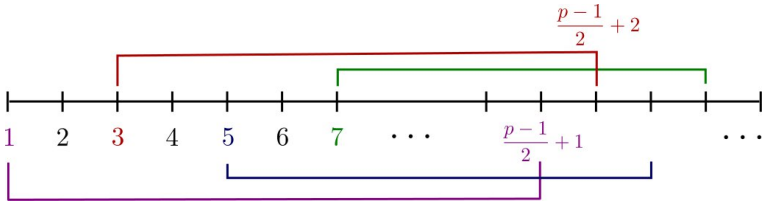

Figura 2.4: Correspondencia dada por la proposición 2.1.2.

De las dos proposiciones anteriores, se obtiene el siguiente corolario cuya interpretación se ilustra en la figura 2.5.

Corolario 2.1.3. *Si $p = 4k+1$ es un número primo, entonces para $n \in \mathbb{Z}$ se cumple*

$$\left(\frac{\frac{p-1}{2}+n}{p}\right) = \left(\frac{\frac{p-1}{2}-(n-1)}{p}\right).$$

Observe que el corolario anterior es equivalente a la simetría elemental.

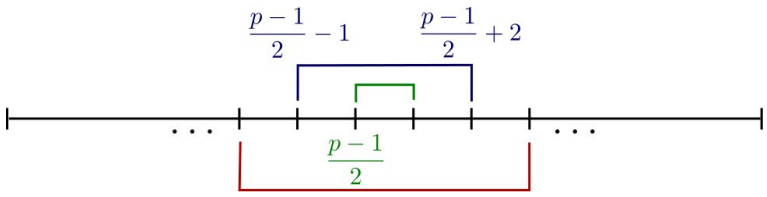

Figura 2.5: Correspondencia dada por el corolario 2.1.3.

2.2. Parejas y ternas

Una consecuencia importante del teorema de Perron (teorema 1.2.1) es que permite obtener el número de parejas de residuos cuadráticos consecutivos en $\mathbb{F}_p$. Más generalmente, se conoce el número de parejas de residuos cuadráticos consecutivos, el de parejas de no residuos cuadráticos consecutivos, así como el número de parejas de la forma residuo seguido de no residuo y viceversa. También se conoce un valor aproximado para el número de ternas de residuos cuadráticos consecutivos en $\mathbb{F}_p$, ver [1]. Sin embargo, en la literatura pocos son los trabajos que dan resultados explícitos acerca de la ocurrencia de parejas y ternas de residuos cuadráticos consecutivos o de no residuos. En [2], A. A. Bennet demuestra la existencia de cadenas de tres residuos cuadráticos consecutivos para $p = 11$ y para cualquier primo p mayor que 17. Bennet primero muestra que la existencia de tres residuos cuadráticos consecutivos es equivalente a la existencia de un cuadrado de la forma $uv(u+v)(u-v)$ y luego construye un cuadrado con dicha forma. H. S. Vandiver hace lo propio en [12], donde para primos congruentes con ciertos valores módulo 40, exhibe sucesiones de tres residuos cuadráticos consecutivos, las cuales obtiene haciendo uso del hecho, que él mismo demuestra, de que para un primo $p = 5k+1$ se cumple que $\left(\frac{a \pm 1}{p}\right) = \left(\frac{-2a}{p}\right)$ y para $p = 5k - 1$ se tiene $\left(\frac{a \pm 1}{p}\right) = -\left(\frac{-2a}{p}\right)$ para un cierto valor de a. Cabe destacar que los métodos de Bennet y Vandiver dan origen a cadenas distintas de tres residuos cuadráticos consecutivos.

En esta sección obtenemos explícitamente algunos patrones de residuos y no residuos para cierto tipo de primos haciendo uso de los resultados de la sección anterior, en particular, se obtiene una nueva cadena de tres residuos cuadráticos consecutivos, con una técnica diferente a las usadas en [2] y [12].

Obsérvese que en la proposición 2.1.1, mientras el parámetro n se mantenga en el intervalo $1 \leq n \leq \lfloor \frac{p-5}{6} \rfloor$, entonces $\frac{p-1}{2} - n$ será mayor que $2n+1$. Si p es de la forma adecuada, entonces hay dos enteros consecutivos que se corresponden vía la

citada proposición como se ilustra en la figura 2.6. Más aún tenemos,

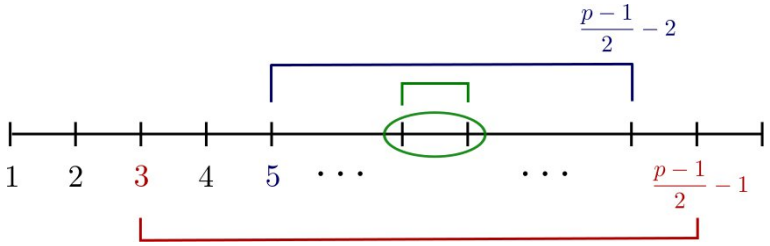

Figura 2.6: Enteros consecutivos correspondientes vía la proposición 2.1.1.

Lema 2.2.1. *Si p es un primo con $p \equiv 1 \mod 4$ y $p \equiv 5 \mod 6$, entonces*

$$\left(\frac{\frac{p-1}{2}-\frac{p-5}{6}}{p}\right) = -1.$$

Demostración. Observe primero que $\left(\frac{p+1}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{\frac{p+1}{3}}{p}\right)$, por lo tanto

$$\left(\frac{\frac{p-1}{2}-\frac{p-5}{6}}{p}\right) = \left(\frac{\frac{p+1}{3}}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{p+1}{p}\right) = \left(\frac{3}{p}\right) = -1$$

porque las hipótesis sobre p implican que $p \equiv 5 \mod 12$, y para primos de esta forma, 3 es un no residuo cuadrático. □

Proposición 2.2.2. *Si $p \equiv 1 \mod 8$ y $p \equiv 5 \mod 6$, entonces*

$$\left(\frac{\frac{p-1}{2}-\frac{p-5}{6}}{p}\right) = \left(\frac{\frac{p-1}{2}-\frac{p-5}{6}-1}{p}\right) = -1.$$

Demostración. Como $p \equiv 1 \mod 8$ entonces $\left(\frac{2}{p}\right) = 1$. Además, vía la proposición 2.1.1, $k = \frac{p-5}{6}$ corresponde con $2k+1 = \frac{p-1}{2} - \frac{p-5}{6} - 1$ lo cual, junto con el lema anterior, da el resultado. □

Notemos que la proposición anterior da la posición exacta de dos no residuos cuadráticos consecutivos módulo un primo $p \equiv 17 \mod 24$, a saber, $\frac{p-2}{3}$ y $\frac{p+1}{3}$.

p	No residuos consecutivos
17	5, 6
41	13, 14
89	29, 30
113	37, 38
1193	397, 398
8369	2789, 2790

Tabla 2.1: Dos no residuos consecutivos para $p \equiv 17 \mod 24$.

En la tabla 2.1 se muestran algunos primos y los no residuos cuadráticos consecutivos módulo p obtenidos vía la proposición 2.2.2.

Por otro lado, si $p \equiv 1 \mod 6$ entonces $\dfrac{p-5}{6}$ no es un entero y en este caso la última pareja de valores que se corresponden vía la proposición 2.1.1 no son enteros consecutivos como se ilustra en la figura 2.7. Los dos resultados siguientes muestran que, con las condiciones adecuadas, esto da tres residuos cuadráticos consecutivos.

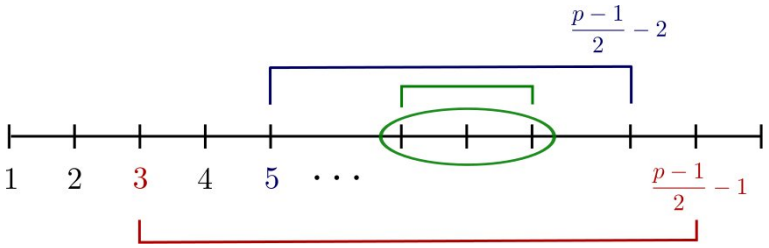

Figura 2.7: Última pareja correspondiente vía la proposición 2.1.1.

Lema 2.2.3. *Si p es un primo con $p \equiv 1 \mod 8$ y $p \equiv 1 \mod 6$, entonces* $\left\lfloor \dfrac{p-5}{6} \right\rfloor = \dfrac{p-7}{6}$ *y*

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6}}{p} \right) = 1.$$

Demostración. Si $p = 6k+1$, entonces $\dfrac{p-5}{6} = (k-1) + \dfrac{1}{3}$ y por lo tanto,

$$\left\lfloor \frac{p-5}{6} \right\rfloor = k - 1 = \frac{p-7}{6}.$$

Ahora, $\dfrac{p-1}{2} - \dfrac{p-7}{6} = \dfrac{p+2}{3}$ y usando el mismo argumento que en la demostración de la proposición 2.1.1 obtenemos que,

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6}}{p}\right) = \left(\frac{\frac{p+2}{3}}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{p+2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1.$$

□

Tenemos entonces que, con las hipótesis del lema anterior, el entero $\dfrac{p-1}{2} - \dfrac{p-7}{6}$ siempre es un residuo cuadrático módulo p, pero vía la proposición 2.1.1, este corresponde con $2\left(\dfrac{p-7}{6}\right) + 1 = \dfrac{p-1}{2} - \dfrac{p-7}{2} - 2$ y por lo tanto, este último también es un residuo cuadrático. Más aún, se tiene la siguiente:

Proposición 2.2.4. *Si* $p \equiv 1 \mod 8$ *y* $p \equiv 1 \mod 6$*, entonces*

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 2}{p}\right) = \left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 1}{p}\right) = \left(\frac{\frac{p-1}{2} - \frac{p-7}{6}}{p}\right) = 1.$$

Demostración. Solo resta ver que $\left(\dfrac{\frac{p-1}{2} - \frac{p-7}{6} - 1}{p}\right) = 1$. Para ello, observe que $\dfrac{p-1}{2} - \dfrac{p-7}{6} - 1 = \dfrac{p-1}{3}$ y por lo tanto

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 1}{p}\right) = \left(\frac{\frac{p-1}{3}}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{p-1}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = 1.$$

□

La proposición anterior permite encontrar, para un primo $p \equiv 1 \mod 24$, tres residuos cuadráticos consecutivos que son $\dfrac{p-4}{3}$, $\dfrac{p-1}{3}$ y $\dfrac{p+2}{3}$.

En la tabla 2.2 se muestran algunos primos y la terna de residuos cuadráticos consecutivos módulo p obtenidos vía la proposición 2.2.4, junto con las ternas obtenidas por Bennet [2] y Vandiver [12]. Todos los primos mostrados son de la forma $p \equiv 1 \mod 120$.

Analizamos ahora lo que ocurre en el caso $p \equiv 5 \mod 8$ para el cual la proposición 2.1.1 dice que,

$$\left(\frac{\frac{p-1}{2} - n}{p}\right) = -\left(\frac{2n+1}{p}\right).$$

El análogo de la proposición 2.2.4 establece en este caso:

p	R consecutivos	R de Bennet	R de Vandiver
3001	999, 1000, 1001	2876, 2877, 2878	244, 245, 246
3121	1039, 1040, 1041	2991, 2992, 2993	1497, 1498, 1499
4201	1399, 1400, 1401	4026, 4027, 4028	2027, 2028, 2029
17761	5919, 5920, 5921	17021, 17022, 17023	7649, 7650, 7651

Tabla 2.2: Tres residuos cuadráticos consecutivos para $p \equiv 1 \pmod{120}$.

Proposición 2.2.5. *Si* $p \equiv 5 \pmod 8$ *y* $p \equiv 1 \pmod 6$, *entonces*

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 2}{p}\right) = \left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 1}{p}\right) = 1$$

y

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6}}{p}\right) = -1.$$

Demostración. Primero notamos que

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6}}{p}\right) = \left(\frac{\frac{p+2}{3}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = -1$$

y como $\dfrac{p-1}{2} - \dfrac{p-7}{6}$ y $\dfrac{p-1}{2} - \dfrac{p-7}{6} - 2$ se corresponden vía la proposición 2.1.1, este último debe ser un residuo cuadrático. Finalmente, tenemos que

$$\left(\frac{\frac{p-1}{2} - \frac{p-7}{6} - 1}{p}\right) = \left(\frac{\frac{p-1}{3}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1,$$

lo cual completa la prueba. □

Notemos que en este caso la proposición anterior nos permite localizar dos residuos cuadráticos consecutivos en lugar de tres como ocurre cuando $p \equiv 1 \pmod 8$.

Ahora establecemos el análogo de la proposición 2.2.2.

Proposición 2.2.6. *Si* $p \equiv 5 \pmod 8$ *y* $p \equiv 5 \pmod 6$, *entonces*

$$\left(\frac{\frac{p-1}{2} - \frac{p-5}{6}}{p}\right) = -1 \quad y \quad \left(\frac{\frac{p-1}{2} - \frac{p-5}{6} - 1}{p}\right) = 1.$$

Demostración. La primera igualdad es cierta pues se tienen las hipótesis del lema 2.2.1 y la segunda se sigue del hecho de que los números involucrados se corresponden vía la proposición 2.1.1 y por tanto los símbolos difieren en signo. □

Este último resultado da la posición exacta de un residuo cuadrático seguido de un no residuo.

A continuación establecemos un resultado que da una correspondencia similar a la de la proposición 2.1.1 pero partiendo de $\frac{p-1}{4}$.

Proposición 2.2.7. *Si* $p \equiv 1 \mod 4$ *es un primo, entonces*

$$\left(\frac{\frac{p-1}{4}+k}{p}\right) = \left(\frac{4k-1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{p-1}{2}-(2k-1)}{p}\right).$$

Demostración. Notamos que $\frac{p-1}{4}+k = \frac{p+4k-1}{4}$, de modo que

$$\left(\frac{\frac{p-1}{4}+k}{p}\right) = \left(\frac{\frac{p+4k-1}{4}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{p+4k-1}{p}\right) = \left(\frac{4k-1}{p}\right).$$

Para la segunda igualdad usamos la proposición 2.1.1

$$\left(\frac{4k-1}{p}\right) = \left(\frac{2(2k-1)+1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{p-1}{2}-(2k-1)}{p}\right).$$

□

En la figura 2.8 se ilustra la correspondencia dada en la proposición anterior.

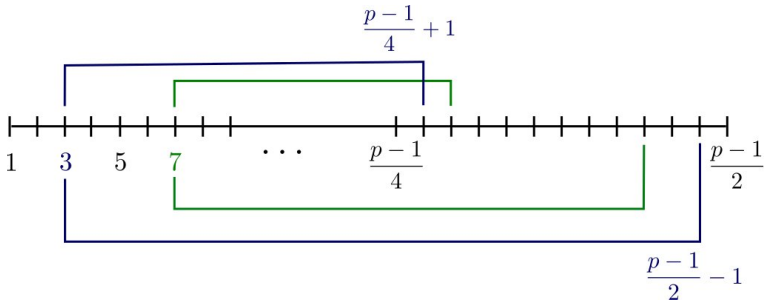

Figura 2.8: Correspondencia dada por la proposición 2.2.7.

CAPÍTULO 3

Trasladados de algunos subconjuntos de R_p y N_p

Como vimos en el primer capítulo, Oskar Perron estudió los trasladados de R_p y N_p logrando determinar la cantidad de residuos cuadráticos que contiene cada trasladado. A continuación estudiamos conjuntos que se obtienen trasladando ciertos subconjuntos de R_p y de N_p buscando generalizar los resultados de Perron para dichos conjuntos.

3.1. Residuos en $R_{\frac{p-1}{2}} + a$

En esta sección estudiaremos el conjunto $R_{\frac{p-1}{2}} = \left\{r \in R_p : 1 \leq r \leq \frac{p-1}{2}\right\}$. Buscamos establecer un resultado análogo al teorema 1.2.1 para $p = 4k + 1$, es decir, queremos determinar la cantidad de residuos cuadráticos y de no residuos cuadráticos en el conjunto $R_{\frac{p-1}{2}} + a = \left\{r + a : r \in R_{\frac{p-1}{2}}\right\}$. Los casos $a = p - 1$ y $a = 1$ pueden resolverse aprovechando que el número de parejas de residuos cuadráticos consecutivos es un valor conocido. Para cualquier valor de a se puede usar una idea más general para contar los residuos cuadráticos en $R_{\frac{p-1}{2}} + a$, la cual consiste en ordenar los elementos de $R_p + a$ en parejas de tal forma que uno de sus elementos esté en $R_{\frac{p-1}{2}} + a$ y el otro no, para luego utilizar el teorema 1.2.1. A continuación mostramos cómo puede hacerse esto [8].

Lema 3.1.1. *Si $p = 4k+1$ es un primo y $r = r_i + a \in R_p + a$ es un residuo cuadrático, entonces $p - r_i$ también es un residuo cuadrático y $p - r_i \in R_p + a$.*

Demostración. Por la simetría elemental r es residuo cuadrático si y solo si $p - r$ lo es. Por lo tanto $(p - r) + a \in R_p + a$ y como $(p - r) + a = p - r_i$ se sigue el resultado. □

A la pareja de residuos cuadráticos en R_p+a dada por $(r_i+a, p-r_i)$ la llamaremos *pareja de residuos correspondiente*. Si además se cumple que $r_i + a < p - r_i$ diremos que $(r_i + a, p - r_i)$ es una *pareja de residuos correspondiente ordenada*. Las parejas correspondientes se ilustran en la figura 3.1.

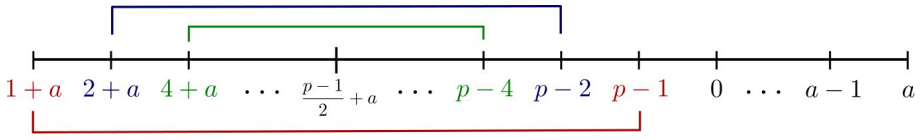

Figura 3.1: Parejas correspondientes en $R_{\frac{p-1}{2}} + a$.

Observamos que conforme r_i recorre los valores $1 \leq r_i < \dfrac{p-a}{2}$, entonces $r_i + a$ recorre los valores $1 + a \leq r_i + a < \dfrac{p-a}{2} + a$ y el correspondiente residuo $p-r_i$ satisface $\dfrac{p-a}{2} + a < p - r_i \leq p - 1$. En particular, para que una pareja correspondiente sea ordenada, se requiere la condición

$$r_i < \frac{p-a}{2}. \tag{3.1}$$

En $R_p^\dagger + a$ eventualmente aparecen algunos de los enteros entre 0 y a, pero para $a \leq \dfrac{p-1}{2}$ estos no están en $R_{\frac{p-1}{2}} + a$. De esta manera, si $r_j = \left\lfloor \dfrac{p-a}{2} \right\rfloor$ es tal que su pareja satisface $p - r_j > \dfrac{p-1}{2} + a$, se tendrá que de los residuos que quedan en $R_p^\dagger + a$, una vez que se han eliminado los residuos entre 0 y a (de negro en la figura 3.1), la mitad son elementos de $R_{\frac{p-1}{2}} + a$ (los que son de la forma $r_i + a$) y la otra mitad no son elementos de $R_{\frac{p-1}{2}} + a$ (las correspondientes parejas $p - r_i$). Por lo tanto, dado que el teorema 1.2.1 dice cuántos residuos cuadráticos hay en $R_p^\dagger + a$, se obtiene el siguiente:

Teorema 3.1.1. *Sean $p = 4k + 1$ un primo, $a \in [\![1, \frac{p-1}{2}]\!]$,*

$$r_j = \text{máx}\left\{ r_i \in R_p : r_i \leq \left\lfloor \frac{p-a}{2} \right\rfloor \ \text{y}\ r_i + a \in R_p \right\},$$

$$S = \{0, 1, \ldots, a-1, a\} \cap (R_p^\dagger + a) = \left\{ i : 0 \leq i \leq a,\ \text{con}\ a - i \in R_p^\dagger \right\}$$

y $s = |S \cap R_p^\dagger|$. Si r_j satisface la condición

$$p - r_j > \frac{p-1}{2} + a, \tag{3.2}$$

entonces se cumplen las siguientes afirmaciones:

1. *Si* $a \in R_p$, *entonces* $\left|(R_{\frac{p-1}{2}}+a)\cap R_p^{\dagger}\right| = \dfrac{k+1-s}{2}$.

2. *Si* $a \in N_p$, *entonces* $\left|(R_{\frac{p-1}{2}}+a)\cap R_p^{\dagger}\right| = \dfrac{k-s}{2}$.

□

Si $\dfrac{p-a}{2}$ es un entero y además es un residuo cuadrático, entonces en el teorema anterior $r_j = \dfrac{p-a}{2}$ y cuando esto ocurre $r_j + a$ y su correspondiente pareja $p - r_j$, coinciden. Sin embargo, en este caso el teorema no es aplicable pues la condición (3.2) no se cumple.

Cuando una pareja correspondiente satisface $r_i + a = p - r_i$, como en la figura 3.2, la llamaremos *traslape*. Observemos que la única manera de que ocurra un traslape es que $r_i = \dfrac{p-a}{2}$ sea un entero y que tanto r_i como $r_i + a$ sean residuos cuadráticos. Bajo esta situación es posible usar básicamente la misma idea para contar los residuos cuadráticos en $R_{\frac{p-1}{2}}+a$ con una ligera modificación: debemos tomar en cuenta el traslape pues con estas condiciones $r_i + a$ está en el conjunto $R_{\frac{p-1}{2}}+a$. Así pues, en presencia de traslape, en el resultado del teorema 3.1.1 debemos restar 1 antes de dividir entre 2 y luego sumar 1.

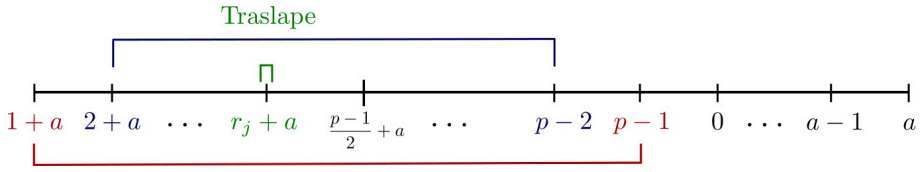

Figura 3.2: Traslape en $R_{\frac{p-1}{2}}+a$.

Además del traslape, existe otra situación que hace que el teorema 3.1.1 no sea aplicable, a saber, que no se cumpla la condición (3.2). Esto significa que existe al menos una pareja correspondiente cuyos elementos están ambos dentro del conjunto $R_{\frac{p-1}{2}}+a$, como se muestra en la figura 3.3. Cuando esto sucede, ambos elementos de la pareja deben ser contados. A una pareja tal la llamaremos *pareja interior*. La modificación que debe hacerse al resultado del teorema 3.1.1 en este caso es clara, sumamos 1 por cada pareja interior que exista.

En síntesis, para un valor de a dado y un primo $p = 4k+1$, si t_a es el número de traslapes (este número solo puede ser 0 o 1) y p_a el número de parejas interiores, se obtiene el siguiente resultado.

Teorema 3.1.2. *Sean* $p = 4k+1$ *un primo,* $a \in [\![1, \frac{p-1}{2}]\!]$ *y* s *como en el teorema* 3.1.1. *Las siguientes afirmaciones son ciertas:*

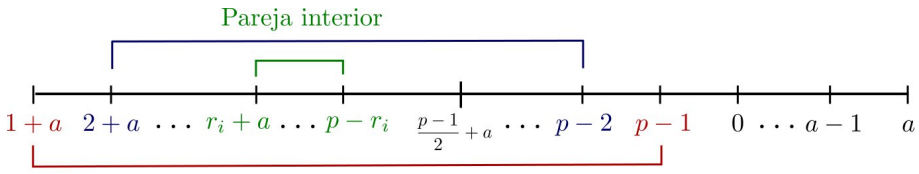

Figura 3.3: Pareja interior en $R_{\frac{p-1}{2}}+a$.

1. *Si* $a \in R_p$, *entonces* $\left|(R_{\frac{p-1}{2}}+a)\cap R_p^{\dagger}\right| = \dfrac{k+1-s-t_a}{2}+t_a+p_a$.

2. *Si* $a \in N_p$, *entonces* $\left|(R_{\frac{p-1}{2}}+a)\cap R_p^{\dagger}\right| = \dfrac{k-s-t_a}{2}+t_a+p_a$.

Para valores particulares de a es posible determinar qué condiciones debe tener el primo p para que se cumplan las hipótesis del teorema 3.1.1 e incluso determinar si ocurre traslape y el número de parejas interiores. A continuación mostramos este proceso para algunos valores de a.

Proposición 3.1.2. *Sea* $p = 4k+1$ *un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si* $p \equiv 1 \pmod 8$, *entonces* $\left|(R_{\frac{p-1}{2}}+1)\cap R_p^{\dagger}\right| = \dfrac{k}{2}$.

2. *Si* $p \equiv 5 \pmod 8$, *entonces* $\left|(R_{\frac{p-1}{2}}+1)\cap R_p^{\dagger}\right| = \dfrac{k-1}{2}$.

Demostración. Si $a = 1$, tenemos $S = \{0,1\}$, $s = 2$ y solo puede ocurrir traslape; este se presenta si $\dfrac{p-1}{2}$ es residuo. Del corolario 1.1.3 esto sucede si y solo si $\left(\dfrac{2}{p}\right) = 1$. Por tanto, del teorema 3.1.2 se sigue el resultado. □

Como consecuencia de la proposición anterior se obtiene, para un primo $p = 4k+1$, el número de parejas de residuos cuadráticos consecutivos en el intervalo discreto $[\![1, \frac{p-1}{2}]\!]$ y también el número de parejas de un residuo cuadrático seguido de un no residuo.

Corolario 3.1.3. *Sea* $p = 4k+1$ *un número primo. El número de parejas de residuos cuadráticos consecutivos en el intervalo* $[\![1, \frac{p-1}{2}]\!]$ *es:*

1. $\dfrac{k-2}{2}$ *si* $p \equiv 1 \pmod 8$.

2. $\dfrac{k-1}{2}$ *si* $p \equiv 5 \pmod 8$.

Corolario 3.1.4. *Sea $p = 4k + 1$ un número primo. El número de parejas de un residuo cuadrático seguido de un no residuo en el intervalo $[\![1, \frac{p-1}{2}]\!]$ es:*

1. $\frac{k}{2}$ *si* $p \equiv 1 \pmod 8$.
2. $\frac{k+1}{2}$ *si* $p \equiv 5 \pmod 8$.

Proposición 3.1.5. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 2) \cap R_p^\dagger\right| = \frac{k}{2}$.
2. *Si* $\left(\frac{2}{p}\right) = 1$ *y* $\left(\frac{3}{p}\right) = -1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 2) \cap R_p^\dagger\right| = \frac{k-2}{2}$.
3. *Si* $\left(\frac{2}{p}\right) = -1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 2) \cap R_p^\dagger\right| = \frac{k-1}{2}$.

Demostración. Si $a = 2$, y en general si a es par, no puede haber traslape porque $\frac{p-a}{2}$ no es un entero. Sin embargo, puede haber una pareja interior si $r_i = \left\lfloor \frac{p-2}{2} \right\rfloor$ y $r_i + 2$ son ambos residuos cuadráticos. Notamos que $r_i = \frac{p-1}{2} - 1$ y por tanto $r_i + 2 = \frac{p-1}{2} + 1$ corresponde con $p - r_i = \frac{p-1}{2}$. Es decir, en este caso la pareja interior consta de enteros consecutivos. Además, de la proposición 2.1.2 se concluye que este caso ocurre si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$. Por otro lado, si $2 \in R_p$, entonces $S = \{0, 1, 2\}$ y $s = 3$. Si $2 \in N_p$, tenemos $S = \{1, 2\}$ de modo que $s = 1$. □

En la tabla 3.1, se muestra el resultado anterior en términos de congruencias módulo 24.

Proposición 3.1.6. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ *y* $\left(\frac{5}{p}\right) = -1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 3) \cap R_p^\dagger\right| = \frac{k-2}{2}$.
2. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 3) \cap R_p^\dagger\right| = \frac{k}{2}$.
3. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 3) \cap R_p^\dagger\right| = \frac{k+1}{2}$.

$\lvert(R_{\frac{p-1}{2}}+2)\cap R_p^{\dagger}\rvert$	p (mód 24)
$\frac{k}{2}$	1
$\frac{k-1}{2}$	5, 13
$\frac{k-2}{2}$	17

Tabla 3.1: Número de residuos cuadráticos en $R_{\frac{p-1}{2}}+2$

4. *Si* $\left(\frac{2}{p}\right)=1, \left(\frac{3}{p}\right)=-1$ *y* $\left(\frac{5}{p}\right)=1$, *entonces* $\left|(R_{\frac{p-1}{2}}+3)\cap R_p^{\dagger}\right|=\frac{k}{2}$.

5. *Si* $\left(\frac{2}{p}\right)=1$ *y* $\left(\frac{3}{p}\right)=\left(\frac{5}{p}\right)=-1$, *entonces* $\left|(R_{\frac{p-1}{2}}+3)\cap R_p^{\dagger}\right|=\frac{k-2}{2}$.

6. *Si* $\left(\frac{2}{p}\right)=-1$ *y* $\left(\frac{3}{p}\right)=1$, *entonces* $\left|(R_{\frac{p-1}{2}}+3)\cap R_p^{\dagger}\right|=\frac{k-1}{2}$.

Demostración. Supongamos $a=3$. Primero notamos que ocurre traslape si $\frac{p-3}{2}$ y $\frac{p-3}{2}+3$ son ambos residuos cuadráticos, y esto sucede si y solo si $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1$. Otra posibilidad es que $r_i=\frac{p-5}{2}=\frac{p-3}{2}-1$ y $r_i+3=\frac{p-1}{2}+1$ sean residuos cuadráticos, en tal caso, una pareja correspondiente consta de r_i+3 y $p-r_i=r_i+5$, es decir, se trata de una pareja interior. Este caso se presenta cuando $\left(\frac{2}{p}\right)=\left(\frac{5}{p}\right)=1$. Observemos que pueden presentarse simultáneamente un traslape y una pareja interior. Con estas consideraciones si $\left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=1$ y $\left(\frac{5}{p}\right)=-1$, entonces $S=\{0,1,2,3\}$ y $s=4$ en el teorema 3.1.1. En este caso ocurre traslape. Por lo tanto, el número de residuos cuadráticos en el conjunto $R_{\frac{p-1}{2}}+3$ es

$$\frac{k+1-s-1}{2}+1=\frac{k-2}{2}.$$

$\lvert(R_{\frac{p-1}{2}} + 3) \cap R_p^{\dagger}\rvert$	$p \pmod{120}$
$\frac{k-2}{2}$	$17, 73, 97, 113$
$\frac{k-1}{2}$	$13, 37, 61, 109$
$\frac{k}{2}$	$1, 41, 49, 89$
$\frac{k+1}{2}$	$29, 53, 77, 101$

Tabla 3.2: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + 3$.

Por otro lado, si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$, el conjunto S es el mismo que en el caso anterior, pero aquí ocurre tanto el traslape como la pareja interior, de manera que $R_{\frac{p-1}{2}} + 3$ contiene

$$\frac{k+1-s-1}{2} + 1 + 1 = \frac{k}{2}$$

residuos cuadráticos. Si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$, solo se presenta el traslape y $S = \{2, 3\}$, así que $s = 0$ y por lo tanto hay

$$\frac{k-s-1}{2} + 1 = \frac{k+1}{2}$$

residuos cuadráticos en $R_{\frac{p-1}{2}} + 3$. Los casos restantes son similares.

□

La proposición anterior puede replantearse en términos de congruencias módulo 120, como se muestra en la tabla 3.2.

El caso $a = 4$ es el primero en el que ocurre más de una pareja interior.

Proposición 3.1.7. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k}{2}$.

2. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$ *y* $\left(\frac{7}{p}\right) = -1$, *entonces*

$$\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-2}{2}.$$

3. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k+1}{2}$.

4. *Si* $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = -1$ *y* $\left(\frac{7}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k}{2}$.

5. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, $\left(\frac{5}{p}\right) = -1$ *y* $\left(\frac{7}{p}\right) = 1$, *entonces*

$$\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-2}{2}.$$

6. *Si* $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = -1$ *y* $\left(\frac{7}{p}\right) = -1$, *entonces*

$$\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-2}{2}.$$

7. *Si* $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-3}{2}$.

8. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$ *y* $\left(\frac{5}{p}\right) = 1$, *entonces* $\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-1}{2}$.

9. *Si* $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ *y* $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = -1$, *entonces*

$$\left|(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\right| = \frac{k-4}{2}.$$

Demostración. Para $a = 4$ no ocurre traslape, sin embargo, puede presentarse más de una pareja interior. Veamos bajo qué condiciones ocurre esto. En primer lugar, notemos que $r_i = \left\lfloor \frac{p-a}{2} \right\rfloor = \frac{p-1}{2} - 2$ y si r_i y r_i+4 son ambos residuos cuadráticos, el entero

$r_i+4=\dfrac{p-1}{2}+2$ corresponde con $p-r_i=\dfrac{p-1}{2}+3$, es decir, se tiene una pareja interior formada por enteros consecutivos. Haciendo uso de la proposición 2.1.1 vemos que $\dfrac{p-1}{2}-2\in R_p$ si y solo si $\left(\dfrac{2}{p}\right)=\left(\dfrac{5}{p}\right)$ y de la proposición 2.1.2 concluimos que $\dfrac{p-1}{2}+2\in R_p$ si y solo si $\left(\dfrac{2}{p}\right)=\left(\dfrac{3}{p}\right)$. Por tanto, si $\left(\dfrac{2}{p}\right)=\left(\dfrac{3}{p}\right)=\left(\dfrac{5}{p}\right)$, se tiene una pareja interior.

Si $r_i=\left\lfloor\dfrac{p-a}{2}\right\rfloor-1$ es un residuo cuadrático, entonces $r_i+4=\dfrac{p-1}{2}+1$ corresponde con $p-r_i=\dfrac{p-1}{2}+4$, lo cual significa que si $r_i=\dfrac{p-1}{2}-3$ y r_i+4 son ambos residuos cuadráticos que constituyen una pareja interior. De la proposición 2.1.1 se tiene que r_i es un residuo cuadrático si y solo si $\left(\dfrac{2}{p}\right)=\left(\dfrac{7}{p}\right)$ y de la proposición 2.1.2 se sigue que r_i+4 es residuo cuadrático si y solo si $\left(\dfrac{2}{p}\right)=1$. Se concluye que cuando $\left(\dfrac{2}{p}\right)=\left(\dfrac{7}{p}\right)=1$ se tiene una pareja interior distinta a la antes considerada.

Finalmente, si el r_j del teorema 3.1.1 satisface $r_j<\dfrac{p-1}{2}-3$, se cumple la condición (3.2) y por tanto no hay parejas interiores, de modo que el teorema 3.1.1 se puede aplicar. Por lo anterior, si

$$\left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=\left(\frac{5}{p}\right)=\left(\frac{7}{p}\right)=1,$$

entonces se presentan dos parejas interiores y así $p_a=2$. Además, en este caso $S=\{0,1,2,3,4\}$ y $s=5$. Por lo tanto, del teorema 3.1.2 se sigue que el número de residuos cuadráticos en $R_{\frac{p-1}{2}}+4$ es $\dfrac{k+1-5}{2}+2=\dfrac{k}{2}$.

Para la afirmación 2, si $\left(\dfrac{2}{p}\right)=\left(\dfrac{3}{p}\right)=\left(\dfrac{5}{p}\right)=1$ y $\left(\dfrac{7}{p}\right)=-1$, solo se presenta una pareja interior y $p_a=1$. El conjunto S es el mismo que en el caso anterior, así que $s=5$ y por tanto el número de residuos cuadráticos en $R_{\frac{p-1}{2}}+4$ es $\dfrac{k+1-5}{2}+1=\dfrac{k-2}{2}$.

Para la afirmación 3, si $\left(\dfrac{2}{p}\right)=\left(\dfrac{3}{p}\right)=\left(\dfrac{5}{p}\right)=-1$, entonces $S=\{0,3,4\}$ por lo que $s=2$, además, solo hay una pareja interior, es decir $p_a=1$, y por lo tanto el número de residuos cuadráticos en $R_{\frac{p-1}{2}}+4$ es $\dfrac{k+1-2}{2}+1=\dfrac{k+1}{2}$.

Los casos restantes se obtienen de la misma forma.

□

La proposición anterior puede plantearse en términos de congruencias módulo 840, tal como se presenta en la tabla 3.3.

En el teorema 3.1.1 se establece la cantidad de residuos cuadráticos en el conjunto $R_{\frac{p-1}{2}} + a$ para ciertos valores de a entre 1 y $\dfrac{p-1}{2}$. A continuación consideramos la posibilidad de trasladar el conjunto $R_{\frac{p-1}{2}}$ por medio de un valor de a mayor que $\dfrac{p-1}{2}$, para ello usamos básicamente la misma idea detrás del teorema 3.1.1. Primeramente notamos que si $a = p - b$ con $b \in [\![1, \frac{p-1}{2}]\!]$, entonces

$$R_p^\dagger + a = \{p-b, p-(b-1), p-(b-2), \ldots, 0, r_i + p - b, \ldots, p - r_i\}$$

y que $0 \in R_p^\dagger + a$ si y solo si $a \in R_p^\dagger$, lo cual ocurre si y solo si $b \in R_p^\dagger$.

Por otro lado, para un residuo cuadrático r_i podemos hacer corresponder al residuo $r_i + a$ con el residuo $p - r_i$, ambos elementos del conjunto $R_p + a$. Si además, r_i satisface $b+1 \leq r_i \leq \dfrac{p+b}{2}$, entonces la pareja de residuos está ordenada. Si $r_i \leq \dfrac{p-1}{2}$, $r_i + a$ está en $R_{\frac{p-1}{2}} + a$ y su pareja satisface

$$\left(\frac{p-1}{2} + b + 1\right) + a \leq p - r_i$$

lo cual significa que $p - r_i \notin R_{\frac{p-1}{2}} + a$. Por lo tanto, hemos organizado algunos de los elementos de $R_p + a$ en parejas de manera que uno de sus miembros está $R_{\frac{p-1}{2}} + a$ y el otro no. Resta considerar los residuos cuadráticos que quedaron fuera, que son los residuos en el conjunto

$$S = \left\{r_i + p - b : r_i \in R_p^\dagger,\ 0 \leq r_i \leq b\right\}.$$

Obsérvese que el conjunto S se puede escribir como sigue

$$S = \left\{-i : 0 \leq i \leq b,\ b - i \in R_p^\dagger\right\},$$

de manera que la cardinalidad de $|S|$ coincide con la cardinalidad del conjunto S definido en el teorema 3.1.1, lo cual significa que el número de residuos cuadráticos en $R_{\frac{p-1}{2}} + a$ que no hemos considerado aún, el cual está dado por $|S \cap R_p^\dagger|$, coincide con el valor de s dado en el teorema 3.1.1. Del argumento anterior y del teorema 1.2.1 se desprende el siguiente,

$\lvert(R_{\frac{p-1}{2}} + 4) \cap R_p^{\dagger}\rvert$	$p \pmod{840}$
$\frac{k-4}{2}$	$73, 97, 313, 433, 577, 817$
$\frac{k-3}{2}$	$13, 37, 61, 109, 157, 181,$ $229, 253, 277, 349, 373, 397,$ $421, 493, 517, 541, 589, 613,$ $661, 709, 733, 757, 781, 829$
$\frac{k-2}{2}$	$17, 41, 89, 193, 209, 241,$ $257, 337, 353, 377, 409, 457,$ $481, 521, 593, 601, 649, 673,$ $689, 697, 713, 761, 769, 793$
$\frac{k-1}{2}$	$29, 101, 149, 221, 269, 341,$ $389, 461, 509, 629, 701, 821$
$\frac{k}{2}$	$1, 113, 121, 137, 169, 233,$ $281, 289, 361, 401, 449, 473,$ $529, 569, 617, 641, 737, 809$
$\frac{k+1}{2}$	$53, 173, 197, 293, 317, 437,$ $533, 557, 653, 677, 773, 797$

Tabla 3.3: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + 4$.

Teorema 3.1.3. *Sean $p = 4k+1$ un número primo y $a = p - b$, con $b \in [\![1, \frac{p-1}{2}]\!]$. Definimos*

$$r_j = \text{máx}\left\{ r_i \in R_p : r_i \leq \left\lfloor \frac{p+b}{2} \right\rfloor \text{ y } r_i - b \in R_p \right\},$$

$$S = \left\{ i : 0 \leq i \leq b, \text{ con } b - i \in R_p^\dagger \right\}$$

y $s = |S \cap R_p^\dagger|$. Si r_j satisface la condición

$$r_j \leq \frac{p-1}{2}, \tag{3.3}$$

entonces se cumplen las siguientes afirmaciones:

1. *Si $b \in R_p$, entonces $\left| R_{\frac{p-1}{2}} + a \cap R_p^\dagger \right| = \dfrac{k+1-s}{2} + (s-1)$.*
2. *Si $b \in N_p$, entonces $\left| R_{\frac{p-1}{2}} + a \cap R_p^\dagger \right| = \dfrac{k-s}{2} + s$.*

Para establecer el resultado análogo al teorema 3.1.2, notemos primero que si $r_i = \dfrac{p+b}{2}$ es un entero y $r_i, r_i + a$ son residuos cuadráticos módulo p, nuevamente ocurre un traslape. Sin embargo, en este caso no debe contarse pues sus componentes están fuera del conjunto $R_{\frac{p-1}{2}} + a$. Por otro lado, si no se cumple la condición (3.3), significa que existe por lo menos una pareja correspondiente cuyas componentes están ambas fuera del conjunto $R_{\frac{p-1}{2}} + a$ y por lo tanto deben dejarse fuera del conteo. A una pareja tal la llamaremos *pareja exterior*. En resumen, si t_a es el número de traslapes y p_a el número de parejas exteriores, se obtiene el siguiente resultado.

Teorema 3.1.4. *Sean $p = 4k+1$ un primo y $a = p - b$, donde $b \in [\![1, \frac{p-1}{2}]\!]$. Las siguientes afirmaciones son ciertas:*

1. *Si $b \in R_p$, entonces $\left| (R_{\frac{p-1}{2}} + a) \cap R_p^\dagger \right| = \dfrac{k+1-s-t_a}{2} - p_a + s - 1$.*
2. *Si $b \in N_p$, entonces $\left| (R_{\frac{p-1}{2}} + a) \cap R_p^\dagger \right| = \dfrac{k-s-t_a}{2} - p_a + s$.*

en donde s es como en el teorema 3.1.3.

A continuación veremos que para un primo $p = 4k+1$, las cantidades t_a y p_a de los teoremas 3.1.1 y 3.1.3 coinciden para a y $p - a$. Es decir, el número de traslapes es el mismo para a y para $p - a$ y el número de parejas interiores para a coincide con el número de parejas exteriores para $p - a$.

Proposición 3.1.8. *Sea $p = 4k+1$ un primo y $a \in [\![1, \frac{p-1}{2}]\!]$. Entonces,*

1. *El número de traslapes es el mismo para a y para $p - a$.*

2. *El número de parejas interiores para a es igual al número de parejas exteriores para $p - a$.*

Demostración. Para que ocurra un traslape para a se requiere que $r_i = \dfrac{p-a}{2}$ y $r_i + a$ sean residuos cuadráticos. Por otro lado, para $p - a$, la condición para que haya un traslape es que $r_i = \dfrac{p+a}{2}$ y $r_i + p - a$ sean ambos residuos. Ambas condiciones se presentan si y solo si $\left(\dfrac{2}{p}\right)\left(\dfrac{a}{p}\right) = 1$. Por lo tanto, el número de traslapes coincide. Ahora, dada una pareja interior $(r_i + a, p - r_i)$ se obtiene la pareja exterior $(r_j + p - a, p - r_j)$, donde $r_j = r_i + a$. En efecto, como

$$p - r_i \leq \frac{p-1}{2} + a,$$

entonces

$$r_j > \frac{p-1}{2}.$$

Recíprocamente, dada una pareja exterior $(r_i + p - a, p - r_i)$, se obtiene la pareja interior $(r_j + a, p - r_j)$, donde $r_j = r_i - a$. Por lo tanto, el número de parajes interiores coincide con el número de parejas exteriores. □

De la proposición anterior se sigue que existe una relación entre el número de residuos cuadráticos en el conjunto $R_{\frac{p-1}{2}} + a$ y el número de residuos cuadráticos en $R_{\frac{p-1}{2}} + (p - a)$.

Corolario 3.1.9. *Si $p = 4k + 1$ es un primo y $a \in [\![1, \frac{p-1}{2}]\!]$, entonces existe $m \in \mathbb{Z}$ tal que*

$$\left|(R_{\frac{p-1}{2}} + a) \cap R_p^{\dagger}\right| = \frac{k-m}{2} \quad y \quad \left|(R_{\frac{p-1}{2}} + (p-a)) \cap R_p^{\dagger}\right| = \frac{k+m}{2}.$$

Más aún, si $a \in R_p$, entonces $m = 2p_a + t_a - s + 1$ y si $a \in N_p$, entonces $m = 2p_a + t_a - s$ donde t_a es el número de traslapes, p_a es número de parejas interiores y s es como en el teorema 3.1.1.

Demostración. Es inmediata de la proposición anterior y los teoremas 3.1.2 y 3.1.4. □

Como consecuencia del corolario anterior, obtenemos el número de residuos cuadráticos en el conjunto $R_{\frac{p-1}{2}} + (p - a)$, para $a = 1, 2, 3, 4$ a partir los valores de la Proposición 3.1.2 y los valores mostrados en las tablas 3.1, 3.2 y 3.3. Los correspondientes resultados se muestran en las tablas 3.4 a la 3.7.

$\lvert(R_{\frac{p-1}{2}} + (p-1)) \cap R_p^{\dagger}\rvert$	$p \pmod 8$
$\frac{k}{2}$	1
$\frac{k+1}{2}$	5

Tabla 3.4: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + (p-1)$.

$\left\lvert(R_{\frac{p-1}{2}} + (p-2)) \cap R_p^{\dagger}\right\rvert$	$p \pmod{24}$
$\frac{k}{2}$	1
$\frac{k+1}{2}$	$5, 13$
$\frac{k+2}{2}$	17

Tabla 3.5: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + (p-2)$.

$\lvert(R_{\frac{p-1}{2}} + (p-3)) \cap R_p^{\dagger}\rvert$	$p \pmod{120}$
$\frac{k+2}{2}$	$17, 73, 97, 113$
$\frac{k+1}{2}$	$13, 37, 61, 109$
$\frac{k}{2}$	$1, 41, 48, 89$
$\frac{k-1}{2}$	$29, 53, 77, 101$

Tabla 3.6: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + (p-3)$.

$\left\lvert(R_{\frac{p-1}{2}} + (p-4)) \cap R_p^{\dagger}\right\rvert$	$p \pmod{840}$
$\frac{k+4}{2}$	$73, 97, 313, 433, 577, 817$
$\frac{k+3}{2}$	$13, 37, 61, 109, 157, 181,$ $229, 253, 277, 349, 373, 397,$ $421, 493, 517, 541, 589, 613,$ $661, 709, 733, 757, 781, 829$
$\frac{k+2}{2}$	$17, 41, 89, 193, 209, 241,$ $257, 337, 353, 377, 409, 457,$ $481, 521, 593, 601, 649, 673,$ $689, 697, 713, 761, 769, 793$
$\frac{k+1}{2}$	$29, 101, 149, 221, 269, 341,$ $389, 461, 509, 629, 701, 821$
$\frac{k}{2}$	$1, 113, 121, 137, 169, 233,$ $281, 289, 361, 401, 449, 473,$ $529, 569, 617, 641, 737, 809$
$\frac{k-1}{2}$	$53, 173, 197, 293, 317, 437,$ $533, 557, 653, 677, 773, 797$

Tabla 3.7: Número de residuos cuadráticos en $R_{\frac{p-1}{2}} + (p-4)$.

3.2. Residuos en $N_{\frac{p-1}{2}} + a$

En esta sección estudiaremos el conjunto $N_{\frac{p-1}{2}} = \left\{n \in N_p : 1 \leq n \leq \frac{p-1}{2}\right\}$. Vamos a establecer un resultado análogo al teorema 1.2.1 para el conjunto $N_{\frac{p-1}{2}} + a$ con $p = 4k + 1$ [7]. De la misma forma en que se hizo en el lema 3.1.1, se puede ver que si $n_i + a$ es un no residuo cuadrático en el conjunto $N_p + a$, entonces $p - n_i$ también lo es y llamaremos a la pareja $(n_i + a, p - n_i)$ una *pareja correspondiente de no residuos cuadráticos*. Si además $n_i + a < p - n_i$, diremos que la pareja está *ordenada*. La condición para que una pareja de no residuos correspondiente sea ordenada es que

$$n_i < \frac{p-a}{2}. \tag{3.4}$$

Al igual que antes, puede ocurrir que una pareja correspondiente tenga entradas iguales y nuevamente la llamamos *traslape*. El traslape ocurre si $\frac{p-a}{2}$ es un entero y un no residuo cuadrático. Finalmente, si

$$n_j = \text{máx}\left\{n_i \in N_p : n_i \leq \left\lfloor \frac{p-a}{2} \right\rfloor \text{ y } n_i + a \in N_p\right\}$$

no cumple la condición

$$p - n_j > \frac{p-1}{2} + a, \tag{3.5}$$

significa que hay por lo menos una pareja correspondiente de no residuos cuadráticos cuyas entradas son ambos elementos del conjunto $N_{\frac{p-1}{2}} + a$ y por lo tanto deben contarse. Al igual que antes, a una pareja tal la llamaremos *pareja interior*.

Siguiendo el mismo razonamiento que se usó para contar residuos en $R_{\frac{p-1}{2}} + a$, se obtiene el siguiente,

Teorema 3.2.1. *Sean $p = 4k + 1$ un primo, $a \in [\![1, \frac{p-1}{2}]\!]$,*

$$S = \{0, 1, \ldots, a-1, a\} \cap (N_p + a) = \{i : 0 \leq i \leq a, \text{ con } a - i \in N_p\}$$

y $s = |S \cap N_p|$. Entonces se cumple que:

1. *Si $a \in R_p$, entonces $|(N_p + a) \cap N_p| = \dfrac{k - s - t_a}{2} + t_a + p_a$.*
2. *Si $a \in N_p$, entonces $|(N_p + a) \cap N_p| = \dfrac{k - 1 - s - t_a}{2} + t_a + p_a$.*

donde t_a es el número de traslapes y p_a el número de parejas interiores que ocurren para estos valores de a y p.

□

A continuación veremos la aplicación del teorema anterior a los casos $a = 1, 2, 3, 4$.

Proposición 3.2.1. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si $p \equiv 1 \mod 8$, entonces $\left|(N_{\frac{p-1}{2}} + 1) \cap N_p\right| = \frac{k}{2}$.*
2. *Si $p \equiv 5 \mod 8$, entonces $\left|(N_{\frac{p-1}{2}} + 1) \cap N_p\right| = \frac{k+1}{2}$.*

Demostración. Si $a = 1$, tenemos $S = \emptyset$ así que $s = 0$ y solo puede ocurrir traslape, el cual se presenta si $\frac{p-1}{2} \in N_p$. Del corolario 1.1.3 esto sucede si y solo si $\left(\frac{2}{p}\right) = -1$ y del teorema 3.2.1 se sigue el resultado. □

Como consecuencia de la proposición anterior, para un primo $p = 4k+1$, obtenemos el número de parejas de no residuos cuadráticos consecutivos en el intervalo discreto $[\![1, \frac{p-1}{2}]\!]$, así como el número de parejas de un no residuo seguido por un residuo.

Corolario 3.2.2. *Sea $p = 4k + 1$ un número primo. El número de parejas de no residuos cuadráticos consecutivos en el intervalo $[\![1, \frac{p-1}{2}]\!]$ coincide con el número de parejas de un no residuo cuadrático seguido de un residuo y está dado por:*

1. $\frac{k}{2}$ *si* $p \equiv 1 \pmod 8$.
2. $\frac{k-1}{2}$ *si* $p \equiv 5 \pmod 8$.

Proposición 3.2.3. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si $\left(\frac{2}{p}\right) = 1$, entonces $\left|(N_{\frac{p-1}{2}} + 2) \cap N_p\right| = \frac{k}{2}$.*
2. *Si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$, entonces $\left|(N_{\frac{p-1}{2}} + 2) \cap N_p\right| = \frac{k-1}{2}$.*
3. *Si $\left(\frac{2}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = 1$, entonces $\left|(N_{\frac{p-1}{2}} + 2) \cap N_p\right| = \frac{k+1}{2}$.*

Demostración. Para este valor de a no ocurre traslape, así que $t_a = 0$. Para la primera afirmación tenemos que si $\left(\frac{2}{p}\right) = 1$, entonces $S = \emptyset$, luego $s = 0$, y no

hay parejas interiores. Del teorema 3.2.1 se sigue que hay $\frac{k-s}{2} = \frac{k}{2}$ no residuos en $N_{\frac{p-1}{2}} + 2$. La segunda y tercera afirmaciones son consecuencia del hecho de que si $n_i = \left\lfloor \frac{p-2}{2} \right\rfloor = \frac{p-1}{2} - 1$ y $n_i + 2 = \frac{p-1}{2} + 1$ son ambos no residuos, entonces hay una pareja interior dada por $(n_i + 2, p - n_i)$, que ocurre si y solo si $\left(\frac{2}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = 1$. □

Proposición 3.2.4. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si $\left(\frac{2}{p}\right) = 1$, entonces $\left|(N_{\frac{p-1}{2}} + 3) \cap N_p\right| = \frac{k}{2}$.*
2. *Si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$ y $\left(\frac{5}{p}\right) = 1$ o si $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = 1$, entonces $\left|(N_{\frac{p-1}{2}} + 3) \cap N_p\right| = \frac{k+1}{2}$.*
3. *Si $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$, entonces $\left|(N_{\frac{p-1}{2}} + 3) \cap N_p\right| = \frac{k-1}{2}$.*
4. *Si $\left(\frac{2}{p}\right) = -1$ y $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$, entonces $\left|(N_{\frac{p-1}{2}} + 3) \cap N_p\right| = \frac{k+3}{2}$.*

Demostración. Observe que en todos los casos $s = 0$. Si $\frac{p-3}{2} \in N_p$, entonces hay traslape, y esto pasa si $\left(\frac{2}{p}\right) \neq \left(\frac{3}{p}\right)$. Por otro lado, si $n_i = \frac{p-1}{2} - 2$ y $n_i + 3 = \frac{p-1}{2} + 1$ son ambos no residuos, se obtiene la pareja interior $(n_i + 3, p - n_i)$. Esto ocurre cuando $\left(\frac{2}{p}\right) = -1$ y $\left(\frac{5}{p}\right) = 1$. Analizando cada caso y usando el teorema 3.2.1 se obtiene el resultado. □

Proposición 3.2.5. *Sea $p = 4k + 1$ un número primo. Las siguientes afirmaciones son ciertas:*

1. *Si $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = 1$ o $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, entonces*

$$\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k}{2}.$$

2. *Si* $\left(\frac{2}{p}\right) = \left(\frac{7}{p}\right) = -1$ *y* $\left[\left(\frac{3}{p}\right) = -1 \text{ o } \left(\frac{5}{p}\right) = -1\right]$, *entonces*

$$\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k-1}{2}.$$

3. *Si* $\left(\frac{2}{p}\right) = -1, \left(\frac{7}{p}\right) = 1$ *y* $\left[\left(\frac{3}{p}\right) = -1 \text{ o } \left(\frac{5}{p}\right) = -1\right]$, *entonces*

$$\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k+1}{2}.$$

4. *Si* $\left(\frac{2}{p}\right) = \left(\frac{7}{p}\right) = -1$ *y* $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = 1$, *entonces*

$$\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k+1}{2}.$$

5. *Si* $\left(\frac{2}{p}\right) = 1$ *y* $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$, *entonces* $\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k+2}{2}$.

6. *Si* $\left(\frac{2}{p}\right) = -1$ *y* $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1$, *entonces*

$$\left|(N_{\frac{p-1}{2}} + 4) \cap N_p\right| = \frac{k+3}{2}.$$

Demostración. Como $a = 4$ es par, no hay traslape así que $t_a = 0$. Pero si $n_i = \left\lfloor \frac{p-4}{2} \right\rfloor = \frac{p-1}{2} - 2$ y $n_i + 4$ son ambos no residuos, se obtiene la pareja interior $(n_i + 4, p - n_i)$. Esto ocurre si y solo si $\left(\frac{2}{p}\right) \neq \left(\frac{5}{p}\right)$ y $\left(\frac{2}{p}\right) \neq \left(\frac{3}{p}\right)$. Si además, $n_i = \left\lfloor \frac{p-4}{2} \right\rfloor - 1 = \frac{p-1}{2} - 3$ y $n_i + 4$ son ambos no residuos, entonces nuevamente $(n_i + 4, p - n_i)$ es una pareja interior, la cual ocurre si y solo si $\left(\frac{2}{p}\right) \neq \left(\frac{7}{p}\right)$ y $\left(\frac{2}{p}\right) = -1$. Finalmente, el conjunto S contiene un no residuo si y solo si $2 \in N_p$. Por lo tanto, en el primer caso se tiene $s = 0$ y $p_a = 0$; en el segundo, $s = 1$ y $p_a = 0$; en el tercer y cuarto casos, $s = 1$ y $p_a = 1$; en el quinto caso, $s = 0$ y $p_a = 1$ y en el sexto caso, $s = 1$ y $p_a = 2$. El resultado se sigue usando el teorema 3.2.1. □

Para contar la cantidad de no residuos en $N_{\frac{p-1}{2}} + a$ para $a = p - b$ con $b \in [\![1, \frac{p-1}{2}]\!]$ usamos exactamente la misma idea que se usó para contar residuos en $R_{\frac{p-1}{2}} + a$, notando que ahora interesa tomar en cuenta todos los no residuos del conjunto S y que en este caso pueden presentarse parejas cuyas componentes estén ambas fuera del conjunto que interesa, las cuales llamamos *parejas exteriores*, se obtiene el siguiente análogo del teorema 3.1.4

Teorema 3.2.2. *Sean $p = 4k + 1$ un primo y $a = p - b$, donde $b \in [\![1, \frac{p-1}{2}]\!]$.*

1. *Si $b \in R_p$, entonces $|(N_p + a) \cap N_p| = \dfrac{k - s - t_a}{2} - p_a + s$.*

2. *Si $b \in N_p$, entonces $|(N_p + a) \cap N_p| = \dfrac{k - 1 - s - t_a}{2} - p_a + s$.*

donde t_a es el número de traslapes, p_a es el número de parejas exteriores y s es como en el teorema 3.2.1.

Al igual que antes, se puede probar que el número de traslapes es el mismo para a y $p - a$ y que el número de parejas interiores para a coincide con el número de parejas exteriores para $p - a$, con lo cual, se obtiene un análogo del corolario 3.1.9 que establece la relación entre la cantidad de no residuos cuadráticos en $N_{\frac{p-1}{2}} + a$ y en $N_{\frac{p-1}{2}} + (p - a)$.

Corolario 3.2.6. *Si $p = 4k+1$ es un primo y $a \in [\![1, \frac{p-1}{2}]\!]$. El número $m = 2p_a + t_a - s$ satisface las siguientes afirmaciones:*

1. *Si $a \in R_p$, entonces*

$$\left|(N_{\frac{p-1}{2}} + a) \cap N_p\right| = \frac{k + m}{2} \quad y \quad \left|(N_{\frac{p-1}{2}} + (p - a)) \cap N_p\right| = \frac{k - m}{2}.$$

2. *Si $a \in N_p$, entonces*

$$\left|(N_{\frac{p-1}{2}} + a) \cap N_p\right| = \frac{k - 1 + m}{2} \quad y \quad \left|(N_{\frac{p-1}{2}} + (p - a)) \cap N_p\right| = \frac{k - 1 - m}{2},$$

donde t_a es el número de traslapes, p_a es número de parejas exteriores y s es como en el teorema 3.2.1.

Como consecuencia del corolario anterior, se obtiene inmediatamente el número de no residuos cuadráticos que hay en $N_{\frac{p-1}{2}} + (p - a)$ para $a = 1, 2, 3, 4$ a partir de las proposiciones 3.2.1-3.2.5. En las tablas 3.8 a la 3.11 se muestra una síntesis de los resultados de esta sección.

$\lvert(N_{\frac{p-1}{2}}+1)\cap N_p\rvert$	$\lvert(N_{\frac{p-1}{2}}+(p-1))\cap N_p\rvert$	$p \pmod 8$
$\frac{k+1}{2}$	$\frac{k-1}{2}$	5
$\frac{k}{2}$	$\frac{k}{2}$	1

Tabla 3.8: Número de no residuos cuadráticos en $N_{\frac{p-1}{2}}+a$, $a=1,p-1$.

$\lvert(N_{\frac{p-1}{2}}+2)\cap N_p\rvert$	$\lvert(N_{\frac{p-1}{2}}+(p-2))\cap N_p\rvert$	$p \pmod{24}$
$\frac{k}{2}$	$\frac{k}{2}$	$1, 17$
$\frac{k-1}{2}$	$\frac{k-1}{2}$	5
$\frac{k+1}{2}$	$\frac{k-3}{2}$	13

Tabla 3.9: Número de no residuos cuadráticos en $N_{\frac{p-1}{2}}+a$, $a=2,p-2$.

$\lvert(N_{\frac{p-1}{2}}+3)\cap N_p\rvert$	$p \pmod{120}$	$\lvert(N_{\frac{p-1}{2}}+(p-3))\cap N_p\rvert$	$p \pmod{120}$
$\frac{k-1}{2}$	$53, 77$	$\frac{k-1}{2}$	$13, 37, 53, 77$
$\frac{k}{2}$	$1, 17, 41, 49,$ $73, 89, 97, 113$	$\frac{k}{2}$	$1, 49, 73, 97$
$\frac{k+1}{2}$	$13, 29, 37, 101$	$\frac{k-2}{2}$	$17, 41, 89, 113$
$\frac{k+3}{2}$	$61, 109$	$\frac{k-3}{2}$	$29, 61, 101, 109$

Tabla 3.10: Número de no residuos cuadráticos en $N_{\frac{p-1}{2}}+a$, $a=3, p-3$.

$\lvert(N_{\frac{p-1}{2}}+4)\cap N_p\rvert$	$\lvert(N_{\frac{p-1}{2}}+(p-4))\cap N_p\rvert$	$p \pmod{840}$
$\frac{k-1}{2}$	$\frac{k+1}{2}$	$13, 101, 157, 173, 269, 293,$ $341, 397, 437, 461, 493, 509,$ $517, 629, 677, 733, 773, 797$
$\frac{k}{2}$	$\frac{k}{2}$	$1, 41, 73, 89, 97, 121,$ $169, 193, 209, 241, 281, 289,$ $313, 337, 361, 401, 409, 433,$ $449, 457, 481, 521, 529, 569,$ $577, 601, 641, 649, 673, 689,$ $697, 761, 769, 793, 809, 817$
$\frac{k+1}{2}$	$\frac{k-1}{2}$	$29, 37, 53, 61, 149, 181,$ $197, 221, 229, 253, 277, 317,$ $349, 373, 389, 533, 557, 613,$ $653, 661, 701, 757, 821, 829$
$\frac{k+2}{2}$	$\frac{k-2}{2}$	$17, 113, 137, 233, 257, 353,$ $377, 473, 593, 617, 713, 737$
$\frac{k+3}{2}$	$\frac{k-3}{2}$	$109, 421, 541, 589, 709, 781$

Tabla 3.11: Número de no residuos cuadráticos en $N_{\frac{p-1}{2}}+a$, $a=4, p-4$.

3.3. Intersecciones de trasladados

El teorema 1.2.1 puede reinterpretarse en términos del número de elementos que tienen en común los conjuntos trasladados $R_p^\dagger + a$. En efecto, para un primo impar p considérense los conjuntos $R_p^\dagger + a$ y $R_p^\dagger + (a+n)$. Observe que $x \in \left(R_p^\dagger + a\right) \cap \left(R_p^\dagger + (a+n)\right)$ si y solo si x satisface

$$x = r_i + a \quad \text{y} \quad x = r_j + (a+n),$$

donde $r_i, r_j \in R_p^\dagger$. Esto es, si existen residuos cuadráticos r_i y r_j que cumplan la relación:

$$r_i = r_j + n,$$

es decir, que el número de elementos en la intersección es el número de veces que la expresión $r_j + n$ con r_j corriendo en el conjunto $R_p^\dagger$ da como resultado un residuo cuadrático. Esto significa que la cardinalidad de la intersección de dos conjuntos trasladados solo depende de n, la diferencia entre los valores de a con que se está trasladando, y es igual a $|R_p^\dagger \cap (R_p^\dagger + n)|$. De lo anterior y el teorema de 1.2.1 se obtiene el siguiente:

Teorema 3.3.1. *Sea p un primo impar y $a, n \in \mathbb{F}_p^*$. Las siguientes afirmaciones son ciertas:*

1. *Si $p = 4k-1$, entonces $\left|\left(R_p^\dagger + a\right) \cap \left(R_p^\dagger + (a+n)\right)\right| = k$.*
2. *Si $p = 4k+1$ y $n \in R_p$, entonces $\left|\left(R_p^\dagger + a\right) \cap \left(R_p^\dagger + (a+n)\right)\right| = k+1$.*
3. *Si $p = 4k+1$ y $n \in N_p$, entonces $\left|\left(R_p^\dagger + a\right) \cap \left(R_p^\dagger + (a+n)\right)\right| = k$.*

Por ejemplo, para $n = 1$ y $n = 2$ en el teorema anterior se obtiene,

Corolario 3.3.1. *Para un primo $p = 4k+1$ se tiene*

$$\left|(R_p^\dagger + a) \cap (R_p^\dagger + (a+1))\right| = k+1.$$

Y si $p \equiv 1 \mod 8$, además

$$\left|(R_p^\dagger + a) \cap (R_p^\dagger + (a+2))\right| = k+1.$$

Observe que cuando $p = 4k-1$, la intersección de cualesquiera dos trasladados de $R_p^\dagger$ tiene siempre la misma cardinalidad, pero si $p = 4k+1$ dicha cardinalidad depende de si la diferencia entre los valores con que se está trasladando es o no un residuo cuadrático módulo p.

Análogamente podemos usar los resultados de la sección 3.1 para estudiar las intersecciones de conjuntos trasladados $R_{\frac{p-1}{2}} + a$ para un primo p. Observe que

para determinar el número de elementos en $\left(R_{\frac{p-1}{2}}+a\right)\cap\left(R_{\frac{p-1}{2}}+(a+n)\right)$ basta considerar $|R_{\frac{p-1}{2}}\cap(R_{\frac{p-1}{2}}+n)|$, esto es, debemos determinar el número de veces que la expresión r_j+n, con r_j un residuo en $R_{\frac{p-1}{2}}$, da como resultado un residuo que también esté en $R_{\frac{p-1}{2}}$. Para $n\leq\dfrac{p-1}{2}$, hacemos esto restándole al número de residuos cuadráticos en $R_{\frac{p-1}{2}}+n$, dado en la sección 3.1, el número de residuos en el conjunto

$$P=\left\{x\in R_{\frac{p-1}{2}}+n : x>\frac{p-1}{2}\right\}.$$

Pero $x=r_j+n\in P$ si

$$\frac{p-1}{2}\geq r_j>\frac{p-1}{2}-n,$$

debemos pues contar, para $j=1,2,\ldots,n$, los residuos $r_j=\dfrac{p-1}{2}-n+j$ tales que $r_j+n=\dfrac{p-1}{2}+j$ también sea un residuo cuadrático, esto es, contamos el número de veces que

$$\left(\frac{\frac{p-1}{2}+j}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{2j-1}{p}\right)=1 \quad \text{y} \tag{3.6}$$
$$\left(\frac{\frac{p-1}{2}-n+j}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{2(n-j)+1}{p}\right)=1$$

para $j=1,2,\ldots,n$.

Observe que $|(R_{\frac{p-1}{2}}+a)\cap(R_{\frac{p-1}{2}}+a+n)|=|(R_{\frac{p-1}{2}}+a)\cap(R_{\frac{p-1}{2}}+a+(p-n))|$, así que es suficiente considerar valores de n menores o iguales que $\dfrac{p-1}{2}$. En las siguientes proposiciones ilustramos los casos $n=1$ y $n=2$.

Proposición 3.3.2. *Para un primo $p=4k+1$ y $a\in\mathbb{F}_p^*$, considérense los conjuntos $R_{\frac{p-1}{2}}+a$ y $R_{\frac{p-1}{2}}+(a+1)$. Entonces*

1. *Si $p\equiv 1 \pmod 8$,* $\left|\left(R_{\frac{p-1}{2}}+a\right)\cap\left(R_{\frac{p-1}{2}}+(a+1)\right)\right|=\dfrac{k-2}{2}$.
2. *Si $p\equiv 5 \pmod 8$,* $\left|\left(R_{\frac{p-1}{2}}+a\right)\cap\left(R_{\frac{p-1}{2}}+(a+1)\right)\right|=\dfrac{k-1}{2}$.

Demostración. De la proposición 3.1.2, sabemos que el número de residuos cuadráticos en $R_{\frac{p-1}{2}}+1$ depende de $p \pmod 8$ y en este caso tenemos $n=1$ y j solo puede valer 1, así

$$\left(\frac{\frac{p-1}{2}+1}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{1}{p}\right)=1 \quad \text{y} \quad \left(\frac{\frac{p-1}{2}}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{1}{p}\right)=1$$

si y solo si $p \equiv 1 \pmod 8$. Se concluye que si $p \equiv 1 \pmod 8$,

$$\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+1)\right)\right| = \frac{k}{2} - 1$$

y si $p \equiv 5 \pmod 8$,

$$\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+1)\right)\right| = \frac{k-1}{2},$$

como se quería. □

Proposición 3.3.3. *Para un primo $p = 4k+1$ y $a \in \mathbb{F}_p^*$, considérense los conjuntos $R_{\frac{p-1}{2}} + a$ y $R_{\frac{p-1}{2}} + (a+2)$. Entonces*

1. *Si $p \equiv 1 \pmod{24}$, $\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+2)\right)\right| = \frac{k-4}{2}$.*
2. *Si $p \equiv 17 \pmod{24}$, $\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+2)\right)\right| = \frac{k-2}{2}$.*
3. *Si $p \equiv 5, 13 \pmod{24}$, $\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+2)\right)\right| = \frac{k-1}{2}$.*

Demostración. Tenemos $n = 2$ y $j = 1, 2$. Si $p \equiv 1 \pmod{24}$, tenemos las hipótesis de la afirmación 1 en la proposición 3.1.5, es decir, $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$. Para $j = 1$ tenemos

$$\left(\frac{\frac{p-1}{2}+1}{p}\right) = \left(\frac{2}{p}\right) = 1 \quad \text{y} \quad \left(\frac{\frac{p-1}{2}-1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1$$

y para $j = 2$

$$\left(\frac{\frac{p-1}{2}+2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \quad \text{y} \quad \left(\frac{\frac{p-1}{2}}{p}\right) = \left(\frac{2}{p}\right) = 1$$

así que

$$\left|\left(R_{\frac{p-1}{2}} + a\right) \cap \left(R_{\frac{p-1}{2}} + (a+2)\right)\right| = \frac{k}{2} - 2.$$

Las afirmaciones 2 y 3 se justifican de manera similar. □

Con estas mismas ideas podemos determinar la cardinalidad de intersecciones de dos trasladados de $N_{\frac{p-1}{2}}$: solo debemos cambiar el 1 en el lado derecho de las igualdades 3.6 por -1. Por ejemplo, para $n = 1$ y $n = 2$ obtenemos los siguientes resultados.

Proposición 3.3.4. *Para un primo $p = 4k+1$ y $a \in \mathbb{F}_p^*$, considérense los conjuntos $N_{\frac{p-1}{2}} + a$ y $N_{\frac{p-1}{2}} + (a+1)$. Entonces*

1. *Si $p \equiv 1 \pmod 8$, $\left|\left(N_{\frac{p-1}{2}} + a\right) \cap \left(N_{\frac{p-1}{2}} + (a+1)\right)\right| = \dfrac{k}{2}$.*
2. *Si $p \equiv 5 \pmod 8$, $\left|\left(N_{\frac{p-1}{2}} + a\right) \cap \left(N_{\frac{p-1}{2}} + (a+1)\right)\right| = \dfrac{k-1}{2}$.*

Proposición 3.3.5. *Para un primo $p = 4k+1$ y $a \in \mathbb{F}_p^*$, considérense los conjuntos $N_{\frac{p-1}{2}} + a$ y $N_{\frac{p-1}{2}} + (a+2)$. Entonces*

1. *Si $p \equiv 1, 17 \pmod{24}$, $\left|\left(N_{\frac{p-1}{2}} + a\right) \cap \left(N_{\frac{p-1}{2}} + (a+2)\right)\right| = \dfrac{k}{2}$.*
2. *Si $p \equiv 5 \pmod{24}$, $\left|\left(N_{\frac{p-1}{2}} + a\right) \cap \left(N_{\frac{p-1}{2}} + (a+2)\right)\right| = \dfrac{k-1}{2}$.*
3. *Si $p \equiv 13 \pmod{24}$, $\left|\left(N_{\frac{p-1}{2}} + a\right) \cap \left(N_{\frac{p-1}{2}} + (a+2)\right)\right| = \dfrac{k-3}{2}$.*

3.4. Residuos en $R_{\frac{p-1}{4}} + a$

Consideremos el conjunto $R_{\frac{p-1}{4}} = \left\{r \in R_p : 1 \leq r_i \leq \frac{p-1}{2}\right\}$. Queremos determinar el número de residuos en $R_{\frac{p-1}{4}} + a = \left\{r + a : r \in R_{\frac{p-1}{4}}\right\}$. Para ello vamos a considerar los elementos de $R_p + a$ en los siguientes cuatro bloques:

$$\begin{aligned}
B_1 &= \left\{r_i + a \in R_p + a : 1 \leq r_i \leq \frac{p-1}{4}\right\}, \\
B_2 &= \left\{r_i + a \in R_p + a : \frac{p-1}{4} < r_i \leq \frac{p-1}{2}\right\}, \\
B_3 &= \left\{r_i + a \in R_p + a : \frac{p-1}{2} < r_i \leq \frac{3(p-1)}{4}\right\}, \\
B_4 &= \left\{r_i + a \in R_p + a : \frac{3(p-1)}{4} < r_i \leq p-1\right\}.
\end{aligned}$$

Hasta ahora hemos estudiado la cantidad de residuos cuadráticos que hay en total en los primeros dos bloques. El interés es ahora contar cuántos residuos cuadráticos hay en el primer bloque.

Recordemos que en $R_p + a$ hemos formado las parejas de residuos cuadráticos correspondientes $(r_i + a, p - r_i)$ de manera que si $1 \leq r_i < \dfrac{p-a}{2}$, entonces $1 + a \leq$

$r_i + a < \dfrac{p-a}{2} + a$ y el residuo correspondiente $p - r_i$ satisface $\dfrac{p-a}{2} + a < p - r_i \leq p - 1$. Con estas condiciones la pareja está ordenada.

Consideramos primero el caso $a = 1$. Notemos que existe una relación entre la cantidad de residuos que hay en el primer bloque y la cantidad de residuos en el cuarto bloque y también entre la cantidad de residuos en el segundo y tercer bloques. Esto es porque, en general, dado un residuo en el primer bloque, su pareja está en el cuarto y la pareja de un residuo en el segundo bloque, en general, está en el tercero. En efecto, si $r_i + a \in R_p + a$ es tal que $r_i \leq \dfrac{p-1}{4}$, entonces su pareja cumple $p - r_i \geq \dfrac{3(p-1)}{4} + 1$, lo cual, significa que la pareja de un residuo en el primer bloque está en el cuarto, excepto si el último elemento en el primer bloque es $\dfrac{p-1}{4} + 1$, en cuyo caso su pareja, $\dfrac{3(p-1)}{4} + 1$, está en el tercer bloque. Para que ocurra esta excepción, se requiere que $\dfrac{p-1}{4} + 1$ sea un residuo cuadrático y para que esto ocurra se debe cumplir que $\left(\dfrac{3}{p}\right) = 1$. Por otro lado, si $r_i + a \in R_p + a$ es tal que $r_i \leq \dfrac{p-1}{2}$, entonces su pareja cumple $p - r_i \geq \dfrac{p-1}{2} + 1$. Esto significa que la pareja de un residuo en el segundo bloque está en el tercero excepto cuando hay traslape, pues en ese caso el residuo que da el traslape tiene a su pareja (él mismo) en el segundo bloque. De la discusión anterior se obtiene la siguiente,

Proposición 3.4.1. *Sean $a = 1$ y B_1, B_2, B_3 y B_4 los bloques en $R_p + a$ definidos antes. Si x es el número de residuos en B_1 y y es el número de residuos en B_2, entonces en B_3 y B_4 hay, respectivamente,*

1. *y y $x + 1$ residuos cuadráticos si $p \equiv 5 \pmod{24}$.*
2. *$y + 1$ y x residuos cuadráticos si $p \equiv 13 \pmod{24}$.*
3. *$y - 1$ y $x + 1$ residuos cuadráticos si $p \equiv 17 \pmod{24}$.*
4. *y y x residuos cuadráticos si $p \equiv 1 \pmod{24}$*

Demostración. Notemos primero que $0 = (p-1) + 1$ es un residuo que está en el cuarto bloque pero que no tiene pareja, así que debe ser contado por separado. Si $p \equiv 5 \pmod{24}$ no hay traslape así que en este caso todos los residuos del primer bloque tienen a su pareja en el cuarto y los del segundo en el tercero y como $0 = (p-1) + 1$ está en el cuarto bloque, se tiene el resultado de la afirmación 1. Si $p \equiv 13 \pmod{24}$, no hay traslape pero $\dfrac{p-1}{4} + 1$ es un residuo cuadrático, esto significa que cada

residuo en el segundo bloque tiene su pareja en el tercero, pero hay un residuo en el primer bloque cuya pareja está también en el tercero, con lo cual, se tiene el resultado de la afirmación 2. Si $p \equiv 17 \pmod{24}$, hay traslape y $\frac{p-1}{4}$ no es un residuo así que cada residuo del primer bloque tiene a su pareja en el cuarto pero hay una pareja del segundo cuya pareja también está en el segundo (el traslape), esto da el resultado de la afirmación 3. Finalmente, si $p \equiv 1 \pmod{24}$ hay traslape y $\frac{p-1}{4}+1$ es un residuo, luego, todos los residuos del primer bloque tienen su pareja en el cuarto, excepto el último cuya pareja está en el tercero y todos los residuos del segundo bloque tiene su pareja en el tercero, excepto el traslape, con lo cual se obtiene el resultado de la afirmación 4. □

Recordemos que en $R_p + (p-a)$ también formamos parejas de residuos con propiedades similares a las que tienen las parejas en $R_p + a$. De esta manera, usando un argumento similar se obtiene la siguiente

Proposición 3.4.2. *Sean $a = p-1$ y B_1, B_2, B_3 y B_4 los bloques en $R_p + a$ definidos antes. Si x es el número de residuos en B_1 y y es el número de residuos en B_2, entonces en B_3 y B_4 hay, respectivamente,*

1. *y y $x-1$ residuos cuadráticos si $p \equiv 5 \pmod{24}$.*
2. *$y-1$ y x residuos cuadráticos si $p \equiv 13 \pmod{24}$.*
3. *$y+1$ y $x-1$ residuos cuadráticos si $p \equiv 17 \pmod{24}$.*
4. *y y x residuos cuadráticos si $p \equiv 1 \pmod{24}$*

Demostración. Considerando que ahora $0 = 1 + (p-1)$ está en el primer bloque y no se le asigna pareja, que el resto de los residuos del primer bloque tienen a su pareja en el cuarto, que los residuos del segundo bloque tienen a su pareja en el tercero, salvo posiblemente uno de ellos, que si $\frac{p-1}{4}+1$ es un residuo entonces $\frac{p-1}{4}$ es un residuo en el segundo bloque cuya pareja, $\frac{3(p-1)}{4}+1$, está en el cuarto y que el traslape, cuando ocurre, está en el tercer bloque, se obtiene el resultado. □

Corolario 3.4.3. *Sean $a = 1$ y n el número de residuos cuadráticos que hay en el conjunto $R_{\frac{p-1}{4}} + a$. Entonces:*

1. *Si $p \equiv 1, 13 \pmod{24}$ en $R_{\frac{p-1}{4}} + (p-a)$ también hay n residuos cuadráticos.*
2. *Si $p \equiv 5, 17 \pmod{24}$ en $R_{\frac{p-1}{4}} + (p-a)$ hay $n+1$ residuos cuadráticos.*

Demostración. Notemos que si $r_i + a$ es un residuo cuadrático en $R_p + a$ entonces $r_i = (r_i + a) + (p - a)$ es un residuo en $R_p + (p - a)$. Y si $1 \leq r_i \leq \dfrac{p-1}{4}$, entonces $2 \leq r_i + a \leq \dfrac{p-1}{4} + a$, es decir, si $r_i + a \in R_{\frac{p-1}{4}} + a$ entonces $r_i \in R_{\frac{p-1}{4}} + (p - a)$ excepto cuando $r_i + 1 = \dfrac{p-1}{4} + 1$ es un residuo cuadrático. Ya vimos que esto ocurre si $p \equiv 1, 13 \mod 24$, esto significa que para este tipo de primos hemos asociado cada uno de los residuos en $R_{\frac{p-1}{4}} + a$ con un residuo en $R_{\frac{p-1}{4}} + (p - a)$ excepto a $\dfrac{p-1}{4} + 1$ cuya pareja no está en el conjunto de interés, pero como $0 \in R_{\frac{p-1}{4}} + (p - a)$ y a este no le hemos asignado pareja, se sigue la primera afirmación. Para la segunda afirmación, vemos que si $p \equiv 5, 17 \mod 24$ entonces $\dfrac{p-1}{4} + 1$ no es un residuo cuadrático así que la asociación dada incluye a todos los residuos cuadráticos de $R_{\frac{p-1}{4}} + a$ y como $0 \in R_{\frac{p-1}{4}} + (p - a)$, este último conjunto tiene un residuo más. $\square$

CAPÍTULO 4

Estimaciones

4.1. Sumas de Hua

La conocida fórmula analítica para el número de clase de Dirichlet establece que en una extensión cuadrática real con discriminante d el número de clase está dado por

$$h_d = \frac{\sqrt{d}}{2\log\varepsilon}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right)_K,$$

donde ε es la unidad fundamental del anillo de enteros algebraicos y $\left(\frac{d}{m}\right)_K$ es el símbolo de Kronecker. En su célebre artículo [5], Hua demuestra que

$$\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right)_K < \frac{1}{2}\log d + 1.$$

Para ello, define la suma $S(n) = \sum_{a=1}^{n}\sum_{m=1}^{a}\left(\frac{d}{m}\right)_K$ y reescribe la serie en la siguiente forma:

$$\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right)_K = \sum_{n=1}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}.$$

Llamaremos a $S(n)$ suma de Hua. En particular si d es un discriminante positivo y $A > d^{1/2}$, la suma de Hua satisface

$$|S(A)| \leq \frac{1}{2}Ad^{1/2}.$$

Esta propiedad permite acotar la serie al considerar la igualdad

$$\sum_{n=1}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}=\sum_{n=1}^{A-1}\frac{2S(n)}{n(n+1)(n+2)}+\sum_{n=A}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}$$

con $A=\lfloor d^{1/2}\rfloor+1$ y notar que

$$|S(n)|\leq\sum_{a=1}^{n}\sum_{m=1}^{a}1=\frac{n(n+1)}{2}.$$

Cuando el discriminante d es un primo $p\equiv 1 \mod 4$, el símbolo de Kronecker y de Legendre coinciden y en este caso la suma de Hua se convierte en:

$$S(n)=\sum_{a=1}^{n}\sum_{m=1}^{a}\left(\frac{m}{p}\right). \tag{4.1}$$

En este capítulo estudiaremos las sumas de Hua y algunas sumas relacionadas con ellas. Mostraremos que $S(n)$ tiene ciertas propiedades que podríamos llamar «simetrías». A menos que se especifique lo contrario, p es un primo de la forma $4k+1$. Comenzaremos encontrando algunos valores en los cuales la suma $S(n)$ se anula.

Proposición 4.1.1. *Si $p=4k+1$ es un primo y $S(n)=\sum_{a=1}^{n}\sum_{m=1}^{a}\left(\frac{m}{p}\right)$, entonces $S(p-2)=S(p-1)=S(p)=0$.*

Demostración. Notemos que

$$S(p)=p\left(\frac{1}{p}\right)+(p-1)\left(\frac{2}{p}\right)+\cdots+2\left(\frac{p-1}{p}\right)+\left(\frac{p}{p}\right).$$

Del corolario 1.1.2 y el teorema 1.1.3 se tiene

$$\begin{aligned}S(p) &= (p+2)\left(\frac{1}{p}\right)+(p-1+3)\left(\frac{2}{p}\right)+\cdots+(\frac{p-1}{2}+\frac{p-1}{2}+1)\left(\frac{\frac{p-1}{2}}{p}\right)\\ &= (p+2)\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)=0\end{aligned}$$

Por otro lado,

$$S(p)=S(p-1)+\sum_{m=1}^{p}\left(\frac{m}{p}\right)=S(p-1)$$

y

$$S(p-1) = S(p-2) + \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = S(p-2),$$

así que $S(p-2) = S(p-1) = S(p) = 0$ □

Proposición 4.1.2. *Si* $n \in [\![1, \frac{p-1}{2} - 1]\!]$, *entonces* $S(n) = S(p-2-n)$.

Demostración. Sea $T(a) = \sum_{m=1}^{a} \left(\frac{m}{p}\right)$. La hipótesis $n \leq \frac{p-1}{2} - 1$ implica que $p - 2 - n > \frac{p-1}{2}$. Así,

$$\begin{aligned} S(p-2-n) &= \sum_{a=1}^{p-2-n} T(a) \\ &= [T(1) + \cdots + T(n)] + [T(n+1) + \cdots + T(p-2-n)] \\ &= S(n) + (p-2-2n)\left[\left(\frac{1}{p}\right) + \cdots + \left(\frac{n+1}{p}\right)\right] \\ &\quad +(p-2-2n-1)\left(\frac{n+2}{p}\right) + \cdots + 2\left(\frac{p-2-n-1}{p}\right) \\ &\quad +\left(\frac{p-2-n}{p}\right). \end{aligned}$$

Puesto que $p = 4k+1$, entre $n+2$ y $p-2-n$ hay un número par de enteros. Por el corolario 1.1.2 los símbolos $\left(\frac{n+2}{p}\right), \ldots, \left(\frac{p-2-n}{p}\right)$ de la suma anterior aparecen por parejas de iguales. Por lo tanto,

$$\begin{aligned} S(p-2-n) &= S(n) + (p-2-2n)\left[\left(\frac{1}{p}\right) + \cdots + \left(\frac{n+1}{p}\right)\right] \\ &\quad +(p-2-2n-1+1)\left(\frac{n+2}{p}\right) \\ &\quad +(p-2-2n-2+2)\left(\frac{n+3}{p}\right) + \cdots + \\ &\quad +(\frac{p-2n-1}{2} + \frac{p-2n-1}{2} - 1)\left(\frac{n+1+\frac{p-2n-3}{2}}{p}\right) \end{aligned}$$

De acuerdo al teorema 1.1.3 concluimos que

$$S(p-2-n) = S(n) + (p-2-2n)\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) = S(n).$$

□

Las sumas $T(a)$ definidas en la demostración de la proposición anterior también presentan cierta simetría.

Proposición 4.1.3. *Sea* $T(a) = \sum_{m=1}^{a} \left(\frac{m}{p}\right)$. *Si* $a \in [\![1, \frac{p-1}{2}]\!]$, *entonces*

$$T(a) = -T(p-(a+1)).$$

Demostración. Tenemos,

$$\begin{aligned} T(p-(a+1)) &= \sum_{m=1}^{p-(a+1)} \left(\frac{m}{p}\right) = \sum_{m=1}^{p-(a+1)} \left(\frac{m}{p}\right) + \sum_{m=p-a}^{p-1} \left(\frac{m}{p}\right) - \sum_{m=p-a}^{p-1} \left(\frac{m}{p}\right) \\ &= \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) - \sum_{m=p-a}^{p-1} \left(\frac{m}{p}\right) \\ &= -\left[\left(\frac{p-a}{p}\right) + \left(\frac{p-a+1}{p}\right) + \left(\frac{p-a+2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right)\right] \\ &= -\left[\left(\frac{a}{p}\right) + \left(\frac{a-1}{p}\right) + \left(\frac{a-2}{p}\right) + \cdots + \left(\frac{1}{p}\right)\right] = -T(a). \end{aligned}$$

□

Notemos que $T(n) = n$ si y solo si $T(j) = j$ para $j \leq n$.

Estamos interesados en estimar $T\left(\frac{p-1}{4}\right)$. Del teorema 1.1.3 se tiene que

$$T\left(\frac{p-1}{4}\right) = -\sum_{i=\frac{p-1}{4}+1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right).$$

Si el primo p es de la forma $p \equiv 5 \mod 8$ y $p \equiv 1 \mod 6$, la correspondencia dada en la proposición 2.2.7 permite cancelar algunos términos en esta suma. Para

ver cuál es el primer término que no se cancela de esta manera, notamos que en este caso el último par que se corresponde consta de números consecutivos y esto ocurre cuando

$$(\frac{p-1}{4}+i)+1=\frac{p-1}{2}-(2i-1),$$

lo cual es cierto si y solo si $i=\dfrac{p-1}{12}$, que es un entero dadas las hipótesis mencionadas antes. Así,

$$\begin{aligned}
-T\left(\frac{p-1}{4}\right) &= \left(\frac{\frac{p-1}{2}-(2i-1-1)}{p}\right)+\left(\frac{\frac{p-1}{2}-(2i-1-3)}{p}\right)+\\
&+ \cdots+\left(\frac{\frac{p-1}{2}-4}{p}\right)+\left(\frac{\frac{p-1}{2}-2}{p}\right)+\left(\frac{\frac{p-1}{2}}{p}\right)\\
&= \left(\frac{\frac{p-1}{2}-(2i-2)}{p}\right)+\left(\frac{\frac{p-1}{2}-(2i-4)}{p}\right)+\\
&+ \cdots+\left(\frac{\frac{p-1}{2}-4}{p}\right)+\left(\frac{\frac{p-1}{2}-2}{p}\right)+\left(\frac{\frac{p-1}{2}}{p}\right), \qquad (4.2)
\end{aligned}$$

esto es,

$$\begin{aligned}
-T\left(\frac{p-1}{4}\right) &= \left(\frac{\frac{p+5}{3}}{p}\right)+\left(\frac{\frac{p+5}{3}+2}{p}\right)+\left(\frac{\frac{p+5}{3}+4}{p}\right)+\\
&+ \cdots+\left(\frac{\frac{p+5}{3}+2(i-2)}{p}\right)+\left(\frac{\frac{p+5}{3}+2(i-1)}{p}\right)
\end{aligned}$$

donde $i=\dfrac{p-1}{12}$. Notemos que la expresión anterior consta de i sumandos y por lo tanto tenemos:

$$\left|T\left(\frac{p-1}{4}\right)\right|\leq\frac{p-1}{12}. \qquad (4.3)$$

Observe que el «numerador» en cada símbolo que aparece en $-T\left(\dfrac{p-1}{4}\right)$ tiene la forma $\dfrac{p+5}{3}+2k$. De la igualdad

$$\frac{p+5}{3}+2k=2\left(\frac{p-1}{6}+k+1\right)$$

se sigue que

$$\left(\frac{\frac{p+5}{3}+2(k-1)}{p}\right)=\left(\frac{2\left(\frac{p-1}{6}+k\right)}{p}\right).$$

Lema 4.1.4. *Si* $p\equiv 1 \mod 4$ *y* $p\equiv 1 \mod 6$, *entonces para cualquier entero* k *se cumple*

$$\left(\frac{2\left(\frac{p-1}{6}+k\right)}{p}\right)=\left(\frac{6k-1}{p}\right).$$

Demostración. La justificación se sigue directamente de observar que

$$\left(\frac{2\left(\frac{p-1}{6}+k\right)}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{6}{p}\right)\left(\frac{p+6k-1}{p}\right)=\left(\frac{6k-1}{p}\right).$$

□

Como consecuencia del resultado anterior tenemos la siguiente proposición que da una nueva correspondencia que se ilustra en la figura 4.1.

Proposición 4.1.5. *Si* $p\equiv 5 \mod 8$ *y* $p\equiv 1 \mod 6$, *entonces para cualquier entero* k *se cumple*

$$\left(\frac{\frac{p-1}{2}-(\frac{p-1}{6}-2k)}{p}\right)=\left(\frac{6k-1}{p}\right)=-\left(\frac{\frac{p-1}{2}-(3k-1)}{p}\right).$$

Demostración. La prueba es directa pues $\left(\frac{2}{p}\right)=-1$ y

$$\left(\frac{6k-1}{p}\right)=\left(\frac{2(3k-1)+1}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{\frac{p-1}{2}-(3k-1)}{p}\right).$$

□

Esta última proposición permite cancelar más términos en la expresión (4.2) pero para que esto ocurra se necesita que $3k-1$ sea par, pues los términos en esta suma son de la forma $\frac{p-1}{2}-n$ con n par, es decir, para tener una nueva cancelación se requiere que k sea un entero impar. Además, se necesita que

$$\frac{p-1}{2}-(\frac{p-1}{6}-2k)\leq\frac{p-1}{2}-(3k-1)$$

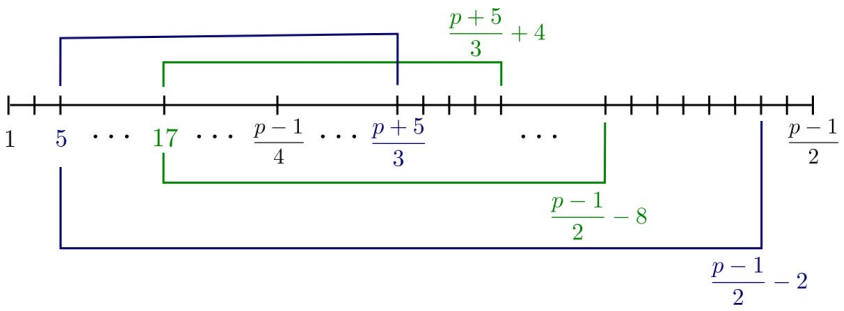

Figura 4.1: Correspondencia dada por la proposición 4.1.5

lo cual es equivalente a la condición $k \leq \dfrac{p+5}{30}$. Por lo tanto, en la expresión de $-T\left(\dfrac{p-1}{4}\right)$ se cancelan $\left\lfloor \dfrac{p+5}{30} \right\rfloor$ términos adicionales [1]. Así, tenemos el siguiente

Teorema 4.1.1. *Si* $p \equiv 5 \mod 8$ *y* $p \equiv 1 \mod 6$, *entonces*

$$\left| T\left(\frac{p-1}{4}\right) \right| \leq \frac{p-1}{12} - \left\lfloor \frac{p}{30} \right\rfloor - 1.$$

Demostración. La afirmación es consecuencia de la discusión previa al teorema y de la observación de que la condición de que p sea un primo con $p \equiv 1 \mod 6$, implica que $\left\lfloor \dfrac{p+5}{30} \right\rfloor = \left\lfloor \dfrac{p}{30} \right\rfloor$. □

A continuación se presentan otro par de propiedades que tienen las sumas $T(a)$.

Proposición 4.1.6. *Si* $k \in [\![1, \frac{p-1}{2}+1]\!]$, *entonces*

$$T\left(\frac{p-1}{2} - k\right) = -\left(\frac{2}{p}\right) T(2k-1) + T(k-1).$$

[1] En realidad, se cancelan $\lfloor \frac{p+5}{30} \rfloor$ términos si esta cantidad es par, lo cual ocurre cuando $p \equiv 1, 13 \mod 15$. Cuando $p \equiv 4, 7 \mod 15$, entonces $\lfloor \frac{p+5}{30} \rfloor$ es impar y en este caso hay $\lfloor \frac{p+5}{30} \rfloor + 1$ cancelaciones.

Demostración. Del teorema 1.1.3 y la proposición 2.1.1 tenemos

$$\begin{aligned} T\left(\frac{p-1}{2}-k\right) &= T\left(\frac{p-1}{2}\right)-\sum_{i=0}^{k-1}\left(\frac{\frac{p-1}{2}-i}{p}\right) \\ &= -\left(\frac{2}{p}\right)\sum_{i=0}^{k-1}\left(\frac{2i+1}{p}\right) \\ &= -\left(\frac{2}{p}\right)\sum_{i=1}^{k}\left(\frac{2i-1}{p}\right) \\ &= -\left(\frac{2}{p}\right)\left[T(2k-1)-\sum_{i=1}^{k-1}\left(\frac{2i}{p}\right)\right] \\ &= -\left(\frac{2}{p}\right)\left[T(2k-1)-\left(\frac{2}{p}\right)\sum_{i=1}^{k-1}\left(\frac{i}{p}\right)\right] \\ &= -\left(\frac{2}{p}\right)T(2k-1)+T(k-1) \end{aligned}$$

□

Proposición 4.1.7. *Si* $k \in [\![1, \frac{p-1}{4}-1]\!]$, *entonces*

$$T\left(\frac{p-1}{4}-k\right) = T\left(\frac{p-1}{4}\right)-\sum_{i=0}^{k-1}\left(\frac{4i+1}{p}\right).$$

Demostración. Puesto que $\left(\frac{\frac{p-1}{4}-k}{p}\right) = \left(\frac{4k+1}{p}\right)$ tenemos

$$T\left(\frac{p-1}{4}-k\right) = T\left(\frac{p-1}{4}\right)-\sum_{i=0}^{k-1}\left(\frac{\frac{p-1}{4}-i}{p}\right) = T\left(\frac{p-1}{4}\right)-\sum_{i=0}^{k-1}\left(\frac{4i+1}{p}\right).$$

□

Consideramos ahora la suma $T_a(n) = \sum_{i=1}^{n}\left(\frac{i+a}{p}\right)$ donde $a \in [\![1, p-1]\!]$ y $n \in \mathbb{N}$. Obsérvese que $i+a$ podría ser cero en cuyo caso $\left(\frac{i+a}{p}\right) = 0$, si lo consideramos como el símbolo de Kronecker.

Podemos determinar el valor de $T_a(n)$ para $n = p-1$, usando los resultados del los teorema 1.2.1 y corolario 1.2.3 de la siguiente manera

$$\begin{aligned} T_a(p-1) &= \sum_{i=1}^{p-1} \left(\frac{i+a}{p}\right) \\ &= \sum_{\substack{i=1 \\ i\in R_p}}^{p-1} \left(\frac{i+a}{p}\right) + \sum_{\substack{i=1 \\ i\in N_p}}^{p-1} \left(\frac{i+a}{p}\right) \\ &= \begin{cases} [(k-1)-k]+[k-k] & \text{si } a \in R_p \\ [k-k]+[k-(k-1)] & \text{si } a \in N_p \end{cases} \\ &= \begin{cases} -1 & \text{si } a \in R_p \\ 1 & \text{si } a \in N_p \end{cases} \end{aligned}$$

Para obtener el valor de las sumas en la expresión anterior usamos los resultados de los citados teoremas, tomando en cuenta que en algunas aparece $i + a = 0$ que es contado como residuo pero que no aporta a las sumas pues el valor del símbolo correspondiente es también 0.

Análogamente, podemos determinar el valor de $T_a(n)$ para $n = \dfrac{p-1}{2}$ y algunos valores de a usando los resultados de las secciones 3.1 y 3.2. Para ello escribimos

$$\begin{aligned} T_a\left(\frac{p-1}{2}\right) &= \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{i+a}{p}\right) \\ &= \sum_{\substack{i=1 \\ i\in R_p}}^{\frac{p-1}{2}} \left(\frac{i+a}{p}\right) + \sum_{\substack{i=1 \\ i\in N_p}}^{\frac{p-1}{2}} \left(\frac{i+a}{p}\right) \end{aligned}$$

La obtención de los valores de estas sumas para $a = 1, 2, 3, 4$ así como para $p - a$ para los mismos valores de a se muestra en las tablas 4.1 a 4.8.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+1}{p}\right)$	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+1}{p}\right)$	$T_1(\frac{p-1}{2})$	p (mód 8)
$\frac{k}{2} - \frac{k}{2} = 0$	$\frac{k}{2} - \frac{k}{2} = 0$	0	1
$\frac{k-1}{2} - \frac{k+1}{2} = -1$	$\frac{k-1}{2} - \frac{k+1}{2} = -1$	-2	5

Tabla 4.1: Valor de $T_a(\frac{p-1}{2})$ para $a = 1$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+2}{p}\right)$	p (mód 24)	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+2}{p}\right)$	p (mód 24)	$T_2(\frac{p-1}{2})$	p (mód 24)
$\frac{k}{2} - \frac{k}{2} = 0$	1	$\frac{k}{2} - \frac{k}{2} = 0$	1,17	0	1,5
$\frac{k-1}{2} - \frac{k+1}{2} = -1$	5,13	$\frac{k+1}{2} - \frac{k-1}{2} = 1$	5		
$\frac{k-2}{2} - \frac{k+2}{2} = -2$	17	$\frac{k-1}{2} - \frac{k+1}{2} = -1$	13	-2	13,17

Tabla 4.2: Valor de $T_a(\frac{p-1}{2})$ para $a = 2$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+3}{p}\right)$	p (mód 120)	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+3}{p}\right)$	p (mód 120)	$T_3(\frac{p-1}{2})$	p (mód 120)
$\frac{k}{2}-\frac{k}{2}=0$	1,41,49,89	$\frac{k}{2}-\frac{k}{2}=0$	1,17,41,49, 73,89,97,113	-4	61,109
$\frac{k-2}{2}-\frac{k+2}{2}=-2$	17,73,97,113	$\frac{k-1}{2}-\frac{k+1}{2}=-1$	13,29,37,101	-2	13,17,37, 73,97,113
$\frac{k-1}{2}-\frac{k+1}{2}=-1$	13,37,61,109	$\frac{k+1}{2}-\frac{k-1}{2}=1$	53,77	0	1,29,41, 49,89,101
$\frac{k+1}{2}-\frac{k-1}{2}=1$	29,53,77,101	$\frac{k-3}{2}-\frac{k+3}{2}=-3$	61,109	2	53,77

Tabla 4.3: Valor de $T_a(\frac{p-1}{2})$ para $a=3$.

$\sum_{i=1, i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+4}{p}\right)$	p (mód 840)	$\sum_{i=1, i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+4}{p}\right)$	p (mód 840)	$T_4(\frac{p-1}{2})$	p (mód 840)
$\frac{k-4}{2} - \frac{k+4}{2} = -4$	$73, 97, 313, 433, 577, 817$	$\frac{k-3}{2} - \frac{k+3}{2} = -3$	109,421,541,589,709,781	-6	109,421,541,589,709,781
$\frac{k-3}{2} - \frac{k+3}{2} = -3$	$13, 37, 61, 109, 157, 181,$ $229, 253, 277, 349, 373, 397,$ $421, 493, 517, 541, 589, 613,$ $661, 709, 733, 757, 781, 829$	$\frac{k+1}{2} - \frac{k-1}{2} = 1$	13,101,157,173,269,293, 341,397,437,461,493,509, 517,629,677,733,773,797	-4	17,37,61,73,97,181, 229,253,257,277,313,349, 353,373,377,433,577,593, 613,661,713,757,817,829
$\frac{k-2}{2} - \frac{k+2}{2} = -2$	$17, 41, 89, 193, 209, 241,$ $257, 337, 353, 377, 409, 457,$ $481, 521, 593, 601, 649, 673,$ $689, 697, 713, 761, 769, 793$	$\frac{k-1}{2} - \frac{k+1}{2} = -1$	29,37,53,61,149,181, 197,221,229,253,277,317, 349,373,389,533,557,613, 653,661,701,757,821,829	-2	13,29,41,89,113,137, 149,157,193,209,221,233, 241,337,389,397,409,457, 473,481,493,517,521,601, 617,649,673,689,697,701, 733,737,761,769,793,821
$\frac{k-1}{2} - \frac{k+1}{2} = -1$	$29, 101, 149, 221, 269, 341,$ $389, 461, 509, 629, 701, 821$	$\frac{k-2}{2} - \frac{k+2}{2} = -2$	17,113,137,233,257,353, 377,473,593,617,713,737		
$\frac{k}{2} - \frac{k}{2} = 0$	$1, 113, 121, 137, 169, 233,$ $281, 289, 361, 401, 449, 473,$ $529, 569, 617, 641, 737, 809$	$\frac{k}{2} - \frac{k}{2} = 0$	1,41,73,89,97,121, 169,193,209,241,281,289, 313,337,361,401,409,433, 449,457,481,521,529,569, 577,601,641,649,673,689, 697,761,769,793,809,817	0	1,53,101,121,169,197, 269,281,289,317,341,361 401,449,461,509,529,533, 557,569,629,641,653,809
$\frac{k+1}{2} - \frac{k-1}{2} = 1$	$53, 173, 197, 293, 317, 437,$ $533, 557, 653, 677, 773, 797$			2	173,293,437,677,773,797

Tabla 4.4: Valor de $T_a(\frac{p-1}{2})$ para $a = 4$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+(p-1)}{p}\right)$	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+(p-1)}{p}\right)$	$T_{p-1}(\frac{p-1}{2})$	p (mód 8)
$\frac{k}{2}-1-\frac{k}{2}=-1$	$\frac{k}{2}-\frac{k}{2}=0$	-1	1
$\frac{k+1}{2}-1-\frac{k-1}{2}=0$	$\frac{k+1}{2}-\frac{k-1}{2}=1$	1	5

Tabla 4.5: Valor de $T_a(\frac{p-1}{2})$ para $a = p-1$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+(p-2)}{p}\right)$	p (mód 24)	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+(p-2)}{p}\right)$	p (mód 24)	$T_{p-2}(\frac{p-1}{2})$	p (mód 24)
$\frac{k}{2}-1-\frac{k}{2}=-1$	1	$\frac{k}{2}-\frac{k}{2}=0$	1,17	-1	1
$\frac{k+1}{2}-\frac{k-1}{2}=1$	5,13	$\frac{k+1}{2}-1-\frac{k-1}{2}=0$	5	1	5,17
$\frac{k+2}{2}-1-\frac{k-2}{2}=1$	17	$\frac{k+3}{2}-1-\frac{k-1-2}{2}=2$	13	3	13

Tabla 4.6: Valor de $T_a(\frac{p-1}{2})$ para $a = p-2$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}} \left(\frac{i+(p-3)}{p}\right)$	p (mód 120)	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}} \left(\frac{i+(p-3)}{p}\right)$	p (mód 120)	$T_{p-3}(\frac{p-1}{2})$	p (mód 120)
$\frac{k}{2}-1-\frac{k}{2}=-1$	1,49	$\frac{k}{2}-\frac{k}{2}=0$	1,49,73,97	-1	1,49,53,77
$\frac{k}{2}-\frac{k}{2}=0$	41,89	$\frac{k+2}{2}-1-\frac{k-1-1}{2}=1$	17,41,89,113	1	13,29,37,41 73,89,97,101
$\frac{k+2}{2}-1-\frac{k-2}{2}=1$	73,97	$\frac{k+1}{2}-\frac{k-1}{2}=1$	13,37		
$\frac{k+2}{2}-\frac{k-2}{2}=2$	17,113	$\frac{k+3}{2}-1-\frac{k-1-2}{2}=2$	29,101	3	17,61,109,113
$\frac{k+1}{2}-1-\frac{k-1}{2}=0$	13,37,61,109	$\frac{k+1}{2}-1-\frac{k-1}{2}=2$	53,77		
$\frac{k-1}{2}-\frac{k+1}{2}=-1$	29,53,77,101	$\frac{k+3}{2}-\frac{k-3}{2}=3$	61,109		

Tabla 4.7: Valor de $T_a(\frac{p-1}{2})$ para $a=p-3$.

$\sum_{i=1,i\in R_p}^{\frac{p-1}{2}}\left(\frac{i+(p-4)}{p}\right)$	p (mód 840)	$\sum_{i=1,i\in N_p}^{\frac{p-1}{2}}\left(\frac{i+(p-4)}{p}\right)$	p (mód 840)	$T_{p-4}(\frac{p-1}{2})$	p (mód 840)
$\frac{k+4}{2}-1-\frac{k-4}{2}=3$	$73,97,313,433,577,817$	$\frac{k+3}{2}-\frac{k-3}{2}=3$	109,421,541,589,709,781	-3	173,293,437,677,773,797
$\frac{k+3}{2}-1-\frac{k-3}{2}=2$	$13,37,61,109,157,181,$ $229,253,277,349,373,397,$ $421,493,517,541,589,613,$ $661,709,733,757,781,829$	$\frac{k-1}{2}-\frac{k+1}{2}=-1$	13,101,157,173,269,293, 341,397,437,461,493,509, 517,629,677,733,773,797	-1	1,53,101,121,169,197, 269,281,289,317,341,361, 401,449,461,509,529,533, 557,569,629,641,653,809
$\frac{k+2}{2}-1-\frac{k-2}{2}=1$	$17,41,89,193,209,241,$ $257,337,353,377,409,457,$ $481,521,593,601,649,673,$ $689,697,713,761,769,793$	$\frac{k+1}{2}-\frac{k-1}{2}=1$	29,37,53,61,149,181, 197,221,229,253,277,317, 349,373,389,533,557,613, 653,661,701,757,821,829	1	13,29,41,89,113,137, 149,157,193,209,221,233, 241,337,389,397,409,457, 473,481,493,517,521,601, 617,649,673,689,697,701, 733,737,761,769,793,821
$\frac{k+1}{2}-1-\frac{k-1}{2}=0$	$29,101,149,221,269,341,$ $389,461,509,629,701,821$	$\frac{k+2}{2}-\frac{k-2}{2}=2$	17,113,137,233,257,353, 377,473,593,617,713,737		
$\frac{k}{2}-1-\frac{k}{2}=-1$	$1,113,121,137,169,233,$ $281,289,361,401,449,473,$ $529,569,617,641,737,809$	$\frac{k}{2}-\frac{k}{2}=0$	1,41,73,89,97,121, 169,193,209,241,281,289, 313,337,361,401,409,433, 449,457,481,521,529,569, 577,601,641,649,673,689, 697,761,769,793,809,817	3	17,37,61,73,97,181, 229,253,257,277,313,349, 353,373,377,433,577,593, 613,661,713,757,817,829
$\frac{k-1}{2}-1-\frac{k+1}{2}=-2$	$53,173,197,293,317,437,$ $533,557,653,677,773,797$			5	109,421,541,589,709,781

Tabla 4.8: Valor de $T_a(\frac{p-1}{2})$ para $a=p-4$.

Conclusiones

En este trabajo se estudiaron dos aspectos importantes de los residuos cuadráticos en $\mathbb{F}_p$ con $p = 4k + 1$: distribución y propiedades aditivas de algunos de sus subconjuntos.

Haciendo uso de la simetría de los residuos cuadráticos para un primo $p \equiv 1$ (mód 4), relacionamos algunos enteros entre 1 y $p - 1$ de manera que ambos son residuos, ambos no residuos o bien si uno es residuo el otro no. Esta relación permitió la obtención de algunos patrones de residuos y no residuos, en particular, se obtuvo para cierto tipo de primos una terna de residuos cuadráticos consecutivos.

Muchos de los trabajos que se encuentran en la literatura que retoman el teorema de Perron, buscan generalizarlo a campos $\mathbb{F}_{p^n}$ y estudian propiedades aditivas de los residuos cuadráticos ahí. Sin embargo, nosotros decidimos trabajar con un enfoque distinto y estudiar subconjuntos de los residuos cuadráticos y sus trasladados en $\mathbb{F}_p$, logrando, a pesar de la manera aleatoria en que parecen presentarse, determinar la cantidad de residuos cuadráticos que hay dichos trasladados. Como consecuencia de lo anterior, obtuvimos el número de parejas de residuos cuadráticos consecutivos, el de parejas de no residuos cuadráticos consecutivos y el número de parejas de un residuo seguido de un no residuo y viceversa que hay en $R_{\frac{p-1}{2}}$ y en $N_{\frac{p-1}{2}}$ y algunos resultados acerca de la cantidad de elementos que hay en la intersección de dos trasladados de este par de conjuntos. Un propósito inmediato es continuar esta parte de la investigación buscando nuevas relaciones como las descritas anteriormente que permitan avanzar en el estudio de trasladados de $R_{\frac{p-1}{4}}$ y $N_{\frac{p-1}{4}}$.

En la parte final del trabajo, estudiamos las sumas de Hua y obtuvimos propiedades que podríamos llamar de simetría. La importancia de estas sumas radica en que están relacionadas con el número de clase en extensiones cuadráticas reales. También usamos la teoría desarrollada en el capítulo 3 para obtener valores explícitos de algunas sumas de símbolos de Legendre. Dichas sumas parecen frías a primera vista, pero tienen una interpretación útil para nuestro propósito futuro y es que ellas nos revelan la cantidad de residuos cuadráticos *versus* la cantidad de residuos no cuadráticos que

hay en ciertos subconjuntos de $\mathbb{F}_p$. Lo anterior debe tener impacto en la suma

$$\sum_{n=1}^{p-1} \frac{1}{n} \left(\frac{n}{p}\right),$$

la cual, puede ser una clave importante en el estudio de la serie $\sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right)$, pues de la simetría $\left(\frac{n}{p}\right) = \left(\frac{n+kp}{p}\right)$ se sigue que $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{n+kp}{p}\right)$ y por tanto

$$\sum_{n=1}^{p-1} \frac{1}{n} \left(\frac{n}{p}\right) > \sum_{n=1}^{p-1} \frac{1}{n+kp} \left(\frac{n+kp}{p}\right).$$

Bibliografía

[1] G. E. Andrews, *Number Theory*, W. B. Saunders Company, 1971.

[2] A. A. Bennet, *On sets of three consecutive integers which are quadratic residues of primes*, Bull. Amer. Math. Soc. Volume 31, Number 8, pp. 411-412, 1925.

[3] B. C. Berndt, *Classical theorems on quadratic residues*, Enseign. Math. 22, pp. 261-304, 1976.

[4] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[5] L. K. Hua, *On the least solution of Pell's equation*, Bull. Amer. Math. Soc 48(10), pp. 731-735, 1942.

[6] J. B. Kelly, *A characteristic property of quadratic residues*, Proc. Amer. Math. Soc. 5, pp. 38-46, 1954.

[7] R. Meza-Moreno, M. Pineda-Ruelas, *Counting Quadratic Nonresidues in Shifted Subsets of the Set of Quadratic Nonresidues for Primes* $p = 4k + 1$, Int. J. Math. Math. Sci., Volume 2015, http://dx.doi.org/10.1155/2015/163092.

[8] R. Meza-Moreno, M. Pineda-Ruelas, *Counting quadratic residues*, JP Journal of Algebra, Number Theory and Applications, 30(1), pp. 151-171, 2013.

[9] H. L. S. Orde, *On Dirichlet's class number formula*, J. London Math. Soc. 18, pp. 409-420, 1978.

[10] O. Perron, *Bemerkungen fiber die Verteilung der quadratischen Reste*, Mathematische Zeitsdarift, Band 56, pp. 122-130, 1952.

[11] G. Soydan, N.Y. Ikikardes, M. Demirci, I.N. Cangul, *On the additive structure of the set of quadratic residues modulo p*, Advanced Studies in Contemporary Math., 14(2), pp. 251-257, 2007.

[12] H. S. Vandiver, *On sets of three consecutive integers which are quadratic or cubic residues of primes*, Bull. Amer. Math. Soc. Volume 31, No. 1-2, pp. 33-38, 1925.

[13] B. A. Wenkov, *Über die Klassenanzahl positiver binärer quadratischer Formen*. Math. Zeitschr., Vol. 33, pp. 350-374, 1931.

[14] A. Winterhof, *On the Distribution of Powers in Finite Fields*. Finite Fields and their Applications **4**, pp. 43-54, 1998.

Índice alfabético

$N_{\frac{p-1}{2}}$, 39
N_p, 1, 8
$R_{\frac{p-1}{2}}$, 23
$R_{\frac{p-1}{4}}$, 50
R_p, 1
$R_p^\dagger$, 5
$S(n)$, 55
$T(a)$, 57
$T_a(n)$, 62
$\left(\frac{-}{p}\right)$, 1
$[\![1, n]\!]$, 1
$\mathbb{F}_p$, 1
$\mathbb{F}_p^*$, 1

pareja de no residuos correspondiente, 39
pareja de residuos correspondiente, 24
pareja exterior, 34, 43
pareja interior, 25, 39

símbolo de Legendre, 1
simetría elemental, 13
Suma de Hua, 55

Teorema
    de Euler, 2
    de Perron, 5
    Pequeño de Fermat, 1
traslape, 25, 34, 39